



Avid® ISIS® Administration Guide

Legal Notices

Product specifications are subject to change without notice and do not represent a commitment on the part of Avid Technology, Inc.

This product is subject to the terms and conditions of a software license agreement provided with the software. The product may only be used in accordance with the license agreement.

This product may be protected by one or more U.S. and non-U.S. patents. Details are available at www.avid.com/patents.

Part of the software embedded in this product is gSOAP software.

Portions created by gSOAP are Copyright (C) 2001-2004 Robert A. van Engelen, Genivia inc. All Rights Reserved.

THE SOFTWARE IN THIS PRODUCT WAS IN PART PROVIDED BY GENIVIA INC AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This document is protected under copyright law. An authorized licensee of Avid ISIS 7000 may reproduce this publication for the licensee's own use in learning how to use the software. This document may not be reproduced or distributed, in whole or in part, for commercial purposes, such as selling copies of this document or providing support or educational services to others. This document is supplied as a guide for Avid ISIS 7000. Reasonable care has been taken in preparing the information it contains. However, this document may contain omissions, technical inaccuracies, or typographical errors. Avid Technology, Inc. does not accept responsibility of any kind for customers' losses due to the use of this document. Product specifications are subject to change without notice.

Copyright © 2014 Avid Technology, Inc. and its licensors. All rights reserved.

The following disclaimer is required by Sam Leffler and Silicon Graphics, Inc. for the use of their TIFF library:

Copyright © 1988–1997 Sam Leffler
Copyright © 1991–1997 Silicon Graphics, Inc.

Permission to use, copy, modify, distribute, and sell this software [i.e., the TIFF library] and its documentation for any purpose is hereby granted without fee, provided that (i) the above copyright notices and this permission notice appear in all copies of the software and related documentation, and (ii) the names of Sam Leffler and Silicon Graphics may not be used in any advertising or publicity relating to the software without the specific, prior written permission of Sam Leffler and Silicon Graphics.

THE SOFTWARE IS PROVIDED "AS-IS" AND WITHOUT WARRANTY OF ANY KIND, EXPRESS, IMPLIED OR OTHERWISE, INCLUDING WITHOUT LIMITATION, ANY WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

IN NO EVENT SHALL SAM LEFFLER OR SILICON GRAPHICS BE LIABLE FOR ANY SPECIAL, INCIDENTAL, INDIRECT OR CONSEQUENTIAL DAMAGES OF ANY KIND, OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER OR NOT ADVISED OF THE POSSIBILITY OF DAMAGE, AND ON ANY THEORY OF LIABILITY, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

The following disclaimer is required by the Independent JPEG Group:

This software is based in part on the work of the Independent JPEG Group.

This Software may contain components licensed under the following conditions:

Copyright (c) 1989 The Regents of the University of California. All rights reserved.

Redistribution and use in source and binary forms are permitted provided that the above copyright notice and this paragraph are duplicated in all such forms and that any documentation, advertising materials, and other materials related to such distribution and use acknowledge that the software was developed by the University of California, Berkeley. The name of the University may not be used to endorse or promote products derived from this software without specific prior written permission. THIS SOFTWARE IS PROVIDED "AS IS" AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

Copyright (C) 1989, 1991 by Jef Poskanzer.

Permission to use, copy, modify, and distribute this software and its documentation for any purpose and without fee is hereby granted, provided that the above copyright notice appear in all copies and that both that copyright notice and this permission notice appear in supporting documentation. This software is provided "as is" without express or implied warranty.

Copyright 1995, Trinity College Computing Center. Written by David Chappell.

Permission to use, copy, modify, and distribute this software and its documentation for any purpose and without fee is hereby granted, provided that the above copyright notice appear in all copies and that both that copyright notice and this permission notice appear in supporting documentation. This software is provided "as is" without express or implied warranty.

Copyright 1996 Daniel Dardailler.

Permission to use, copy, modify, distribute, and sell this software for any purpose is hereby granted without fee, provided that the above copyright notice appear in all copies and that both that copyright notice and this permission notice appear in supporting documentation, and that the name of Daniel Dardailler not be used in advertising or publicity pertaining to distribution of the software without specific, written prior permission. Daniel Dardailler makes no representations about the suitability of this software for any purpose. It is provided "as is" without express or implied warranty.

Modifications Copyright 1999 Matt Koss, under the same license as above.

Copyright (c) 1991 by AT&T.

Permission to use, copy, modify, and distribute this software for any purpose without fee is hereby granted, provided that this entire notice is included in all copies of any software which is or includes a copy or modification of this software and in all copies of the supporting documentation for such software.

THIS SOFTWARE IS BEING PROVIDED "AS IS", WITHOUT ANY EXPRESS OR IMPLIED WARRANTY. IN PARTICULAR, NEITHER THE AUTHOR NOR AT&T MAKES ANY REPRESENTATION OR WARRANTY OF ANY KIND CONCERNING THE MERCHANTABILITY OF THIS SOFTWARE OR ITS FITNESS FOR ANY PARTICULAR PURPOSE.

This product includes software developed by the University of California, Berkeley and its contributors.

The following disclaimer is required by Paradigm Matrix:

Portions of this software licensed from Paradigm Matrix.

The following disclaimer is required by Ray Sauers Associates, Inc.:

"Install-It" is licensed from Ray Sauers Associates, Inc. End-User is prohibited from taking any action to derive a source code equivalent of "Install-It," including by reverse assembly or reverse compilation, Ray Sauers Associates, Inc. shall in no event be liable for any damages resulting from reseller's failure to perform reseller's obligation; or any damages arising from use or operation of reseller's products or the software; or any other damages, including but not limited to, incidental, direct, indirect, special or consequential Damages including lost profits, or damages resulting from loss of use or inability to use reseller's products or the software for any reason including copyright or patent infringement, or lost data, even if Ray Sauers Associates has been advised, knew or should have known of the possibility of such damages.

The following disclaimer is required by Videomedia, Inc.:

"Videomedia, Inc. makes no warranties whatsoever, either express or implied, regarding this product, including warranties with respect to its merchantability or its fitness for any particular purpose."

"This software contains V-LAN ver. 3.0 Command Protocols which communicate with V-LAN ver. 3.0 products developed by Videomedia, Inc. and V-LAN ver. 3.0 compatible products developed by third parties under license from Videomedia, Inc. Use of this software will allow "frame accurate" editing control of applicable videotape recorder decks, videodisc recorders/players and the like."

The following disclaimer is required by Altura Software, Inc. for the use of its Mac2Win software and Sample Source Code:

©1993–1998 Altura Software, Inc.

The following disclaimer is required by Interplay Entertainment Corp.:

The "Interplay" name is used with the permission of Interplay Entertainment Corp., which bears no responsibility for Avid products.

This product includes portions of the Alloy Look & Feel software from Incors GmbH.

This product includes software developed by the Apache Software Foundation (<http://www.apache.org/>).

© DevelopMentor

This product may include the JCifs library, for which the following notice applies:

JCifs © Copyright 2004, The JCIFS Project, is licensed under LGPL (<http://jcifs.samba.org/>). See the LGPL.txt file in the Third Party Software directory on the installation CD.

Avid Interplay contains components licensed from LavanTech. These components may only be used as part of and in connection with Avid Interplay.

Attn. Government User(s). Restricted Rights Legend

U.S. GOVERNMENT RESTRICTED RIGHTS. This Software and its documentation are "commercial computer software" or "commercial computer software documentation." In the event that such Software or documentation is acquired by or on behalf of a unit or agency of the U.S. Government, all rights with respect to this Software and documentation are subject to the terms of the License Agreement, pursuant to FAR §12.212(a) and/or DFARS §227.7202-1(a), as applicable.

Trademarks

003, 192 Digital I/O, 192 I/O, 96 I/O, 96i I/O, Adrenaline, AirSpeed, ALEX, Alienbrain, AME, AniMatte, Archive, Archive II, Assistant Station, AudioPages, AudioStation, AutoLoop, AutoSync, Avid, Avid Active, Avid Advanced Response, Avid DNA, Avid DNxcel, Avid DNxHD, Avid DS Assist Station, Avid Ignite, Avid Liquid, Avid Media Engine, Avid Media Processor, Avid MEDIArray, Avid Mojo, Avid Remote Response, Avid Unity, Avid Unity ISIS, Avid VideoRAID, AvidRAID, AvidShare, AVIDstripe, AVX, Beat Detective, Beauty Without The Bandwidth, Beyond Reality, BF Essentials, Bomb Factory, Bruno, Cj24, CaptureManager, ChromaCurve, ChromaWheel, Cineractive Engine, Cineractive Player, Cineractive Viewer, Color Conductor, Command|24, Command|8, Control|24, Cosmonaut Voice, CountDown, d2, d3, DAE, D-Command, D-Control, Deko, DekoCast, D-Fi, D-fx, Digi 002, Digi 003, DigiBase, Digidesign, Digidesign Audio Engine, Digidesign Development Partners, Digidesign Intelligent Noise Reduction, Digidesign TDM Bus, DigiLink, DigiMeter, DigiPanner, DigiProNet, DigiRack, DigiSerial, DigiSnake, DigiSystem, Digital Choreography, Digital Nonlinear Accelerator, DigiTest, DigiTranslator, DigiWear, DINR, DNxchange, Do More, DPP-1, D-Show, DSP Manager, DS-StorageCalc, DV Toolkit, DVD Complete, D-Verb, Eleven, EM, Euphonix, EUCON, EveryPhase, Expander, ExpertRender, Fader Pack, Fairchild, FastBreak, Fast Track, Film Cutter, FilmScribe, Flexevent, FluidMotion, Frame Chase, FXDeko, HD Core, HD Process, HDpack, Home-to-Hollywood, HYBRID, HyperSPACE, HyperSPACE HDCAM, iKnowledge, Image Independence, Impact, Improv, iNEWS, iNEWS Assign, iNEWS ControlAir, InGame, Instantwrite, Instinct, Intelligent Content Management, Intelligent Digital Actor Technology, IntelliRender, Intelli-Sat, Intelli-sat Broadcasting Recording Manager, InterFX, Interplay, InTONE, Intraframe, iS Expander, iS9, iS18, iS23, iS36, ISIS, IsoSync, LaunchPad, LeaderPlus, LFX, Lightning, Link & Sync, ListSync, LKT-200, Lo-Fi, MachineControl, Magic Mask, Make Anything Hollywood, make manage move | media, Marquee, MassivePack, Massive Pack Pro, Maxim, Mbox, Media Composer, MediaFlow, MediaLog, MediaMix, Media Reader, Media Recorder, MEDIArray, MediaServer, MediaShare, MetaFuze, MetaSync, MIDI I/O, Mix Rack, Moviestar, MultiShell, NaturalMatch, NewsCutter, NewsView, NewsVision, Nitris, NL3D, NLP, NSDOS, NSWIN, OMF, OMF Interchange, OMM, OnDVD, Open Media Framework, Open Media Management, Painterly Effects, Palladium, Personal Q, PET, Podcast Factory, PowerSwap, PRE, ProControl, ProEncode, Profiler, Pro Tools, Pro Tools|HD, Pro Tools LE, Pro Tools M-Powered, Pro Transfer, QuickPunch, QuietDrive, Realtime Motion Synthesis, Recti-Fi, Reel Tape Delay, Reel Tape Flanger, Reel Tape Saturation, Reprise, Res Rocket Surfer, Reso, RetroLoop, Reverb One, ReVibe, Revolution, rS9, rS18, RTAS, Salesview, Sci-Fi, Scorch, ScriptSync, SecureProductionEnvironment, Serv|GT, Serv|LT, Shape-to-Shape, ShuttleCase, Sibelius, SimulPlay, SimulRecord, Slightly Rude Compressor, Smack!, Soft SampleCell, Soft-Clip Limiter, SoundReplacer, SPACE, SPACESHift, SpectraGraph, SpectraMatte, SteadyGlide, Streamfactory, Streamgenie, StreamRAID, SubCap, Sundance, Sundance Digital, SurroundScope, Symphony, SYNC HD, SYNC I/O, Synchronic, SynchroScope, Syntax, TDM FlexCable, TechFlix, Tel-Ray, Thunder, TimeLiner, Titansync, Titan, TL Aggro, TL AutoPan, TL Drum Rehab, TL EveryPhase, TL Fauxlder, TL In Tune, TL MasterMeter, TL Metro, TL Space, TL Utilities, tools for storytellers, Transit, TransJammer, Trillium Lane Labs, TruTouch, UnityRAID, Vari-Fi, Video the Web Way, VideoRAID, VideoSPACE, VTEM, Work-N-Play, Xdeck, X-Form, Xmon and XPAND! are either registered trademarks or trademarks of Avid Technology, Inc. in the United States and/or other countries.

Apple, Macintosh, and Safari are either registered trademarks or trademarks of Apple Computer, Inc., registered in the U.S. and other countries. HP is a registered trademark of Hewlett-Packard Company. Intel is a registered trademark of Intel Corporation. Java is a trademark of Sun Microsystems in the United States and/or other countries. Kingston is a registered trademarks of Kingston Technology Corporation. All other marks may be the property of their respective titleholders. Windows is either a registered trademark or trademark of Microsoft Corporation in the United States and/or other countries. All other trademarks contained herein are the property of their respective owners.

Avid ISIS Administration Guide • 0175-30980-00 Rev. D • July 2014 • Created 7/2/14

Contents

	Using This Guide	12
	Who Should Use This Guide	12
	Symbols and Conventions	12
	If You Need Help	13
	Accessing the Online Documentation	13
	Avid Training Services	13
Chapter 1	Working with the Avid ISIS Management Console	15
	ISIS Nomenclature Used in this Guide	15
	Before Performing Administrative Functions	15
	Opening the Management Console	15
	Using the Management Console Interface	17
	System Status Console	17
	System Status Console Panels	18
	Navigation Toolbar	20
	Accessing Help	20
	Session Counter	21
	Main Tools Panel	21
	Organizing Display Information	23
	Moving Columns	23
	Showing and Hiding Columns	24
	Sorting Information	24
	Filtering the Display	24
	Updating Information	25
	Selecting Items	26
	Using Context Menus to Perform Actions	26
	Entering Text	26
Chapter 2	Configuring the Management Console	28
	Configuring Management Console Preferences	28
	Creating a Log of File Deletions	29
	Changing the Administrator Password	29
	Configuring External Authentication	30
	Configuring the Notification Service	31
	Starting, Stopping, and Configuring the Notification Service	31
	Configuring Error Notification Parameters	32

	Configuring Contact Information	32
Chapter 3	Managing Avid ISIS Hardware	33
	Managing Storage Managers	33
	Storage Manager Column List	34
	Viewing Storage Manager Details	35
	Storage Manager Status	36
	Binding Storage Managers to the ISIS File System	38
	Unbinding Storage Managers from the ISIS File System	38
	Clearing Network Degraded Status Messages	39
	Upgrading Storage Managers	39
	Removing Storage Managers from the ISIS 7500 Shared Storage Network	39
	Identifying the ISIS 7500 Storage Managers Prior to Removal	41
	Preparing to Remove Storage Managers from the Avid ISIS Engine	41
	Removing Orphaned Storage Managers	42
	Initiate Block Rectify	43
	Managing ISIS 7500 Switch Blades	43
	ISIS 7500 Switch Blades Column List	43
	Viewing ISIS 7500 Switch Blade Details	44
	Upgrading ISIS 7500 Switch Blades	44
	Managing the Engine	45
	Engine Column List	45
	Engine Details	46
	Removing Engines from the Engine List	46
	Upgrading ISIS 7500 Engine Components	47
	Upgrading Individual ISIS 7500 Engine Components	47
Chapter 4	Avid ISIS Control Panels	49
	ISIS Launch Pad	49
	Opening ISIS Launch Pad	50
	Minimizing or Closing the ISIS Launch Pad	51
	ISIS Launch Pad Buttons	51
	Using Storage Manager Memory Log Viewer	52
	Avid ISIS System Director Control Panel	52
	Opening the System Director Control Panel	52
	Starting and Stopping the System Director Service	54
	Changing the System Director Virtual Name	55
	Monitoring System Director Status	55
	System Director Status Indicators	56
	Using the ISIS System Director Memory Log Viewer	56
	Working with File System Operations	56
	Reconfiguring the File System	57

	Creating or Re-creating a File System	57
	Monitoring Metadata Status	57
	Creating a Metadata Dump File.	58
	Resetting the Administrator Password	59
	Managing Active Clients	59
Chapter 5	Managing Storage Groups and Workspaces	61
	Managing Storage Groups	61
	Storage Groups List	62
	Viewing Storage Group and Storage Manager Details	62
	Storage Groups on ISIS 7500	63
	Storage Groups and Chunk Sizes	63
	Storage Managers and Chunk Sizes	63
	RAID-6 Workspace, Single ISB Failure	63
	RAID-6 Workspace, Dual ISB Failure	63
	Mirrored Workspace, Single ISB Failure	64
	Matching Chunk Sizes to the File System	64
	Zone 1 Switches	64
	Storage Groups on ISIS 5500 and ISIS 2500	64
	Adding Storage Managers to Storage Groups	65
	Creating New Storage Groups	65
	Removing ISIS Storage Managers from Storage Groups	66
	Adding Storage Managers from Another Storage Group	67
	Adding Storage Managers From Another Environment (ISIS 7500)	68
	Deleting Storage Groups	68
	Minimum Free Storage Space Requirement	69
	Managing Workspaces	69
	Workspaces List	70
	Workspace Considerations	71
	Workspace Data Protection (ISIS 7500 only)	71
	Workspace Creation (ISIS 7500)	71
	Workspace Duplication (ISIS 7500)	72
	Workspace Moves (ISIS 7500)	72
	Using the Workspace Size Graph	72
	Viewing Workspace Details	73
	Adding New Workspaces	74
	Duplicating Workspaces	75
	Renaming Workspaces	75
	Protecting ISIS 7500 Workspaces	76
	Setting ISIS 7500 Workspace Protection	76
	Moving Workspaces	77

	Resizing Workspaces	78
	Setting Event Triggers	78
	Deleting Workspaces	79
	Managing Workspace Access Privileges	80
	Setting Workspace Access Privileges	81
	Redistributing Data	81
	Configuration Changes	81
	Redistribution Guidelines	82
	Symmetric Configuration Redistribution	83
	Automatic Redistribution on Disk Failure	83
	Workspace Redistribution Batching	84
	Performing a Full Redistribution	84
	Suspending and Resuming Redistribution	85
	Redistribution Status Definitions	86
	Monitoring Redistributions	87
Chapter 6	Managing Clients	90
	Managing Users	90
	User Column List	91
	Viewing User Details	92
	Adding Users	93
	Duplicating Users	94
	Modifying Users	94
	Deleting Users	95
	Disabling Users	96
	Managing User Groups	96
	Viewing User Group Details	97
	Adding User Groups	98
	Modifying User Groups	98
	Deleting User Groups	99
	Managing LDAP Accounts	99
	Opening LDAP Sync Tool	100
	Using LDAP Sync Tool	101
	Modifying the Account Synchronizer Display	101
	Synchronizing LDAP and ISIS Accounts	102
	Importing LDAP Users with Incorrectly Formatted LDAP UIDs	104
	Connecting and Disconnecting from the ISIS and LDAP servers	105
	Managing Devices	106
	Devices Column List	107
	Viewing Device Details	107
	Adding Devices	107

	Modifying Devices	108
	Deleting Devices	108
Chapter 7	Managing Connections	110
	Monitoring Client Bandwidth	110
	Opening the Bandwidth Page.	111
	Bandwidth List	111
	Scaling the Bandwidth List Graph Display	111
	Monitoring System Connection Status	111
	Opening the Connection Status Page	112
	Connection Status Descriptions	112
	Disconnecting Clients from the Shared Storage Network	113
	Monitoring Reservations	113
	Reservations Descriptions	114
	Revoking Reservations	114
Chapter 8	System Monitoring and Diagnostics	115
	Hardware Monitoring Service	115
	System Information Page	116
	System and Administration Log Pages	118
	Using the Administration Logs	118
	Using the System Logs Page.	119
	Viewing System Logs	119
	Clearing System Logs	119
	ISIS Snapshots Page	120
	Creating, Viewing, and Deleting Snapshots	120
	Working with Snapshot Archives	121
	Profiler Page	122
	System Status History Page	122
	ISIS Toolbox	123
	Connection Analyzer Tool	123
	Log Aggregator Tool.	125
	LSI Log Aggregator	125
	Using the Log Aggregator Tool	125
	Creating Aggregate Logs.	126
	Viewing Aggregate Logs	127
	Disk Analyzer Tool	127
	Opening the Disk Analyzer Tool	127
	Updating the Disk Analyzer Tool Display	128
	Running Disk Analyzer Tool Tests	128
	Saving Disk Analyzer Test Results	129
	Storage Manager Parameters Tool	129

Using the Storage Manager Parameters	129
Retrieve Storage Manager Flag Parameters	130
Switch Manager Tool (ISIS 7500)	130
Network Utilities Page	131
Monitor Tool (ISIS 7500)	132
Accessing the Monitor Tool	133
Configuring the Monitor Tool	133
Viewing Information in the Monitor Tool	134
Displaying Rack Configurations in Separate Windows	136
Understanding the Monitor Tool Views	136
Using System View	136
Using Status Details View	137
Status Indicators	137
Using Blade Identification View	138
Using Temperatures View	138
Using Upgrades View	138
Agent Settings Page	139
Monitoring Avid ISIS with SNMP	139
Appendix A Avid ISIS Storage Manager Agent	141
Opening the Avid ISIS Storage Manager Agent	141
Effect of Changing the Agent SSL Setting	141
Understanding the Agent Interface	142
System Tab	143
Statistics Tab	145
Tools Tab	146
Logging Tab	146
Advanced Tab	147
Managing Storage Manager Agent Profiles (ISIS 5500)	148
Creating New Storage Manager Agent Profiles	148
Viewing Storage Manager Agent Profiles	149
Deleting Agent Profiles	149
Changing the Agent Administrator Password (ISIS 5500 and 2000 only)	149
Storage Manager Logging	150
Using Storage Manager Agent Logging	150
Viewing Agent Event Logs	150
Clearing Agent Event Logs	151
Resetting the Storage Manager Status (ISIS 2500)	151
Enabling and Disabling Storage Manager Logging	152
Saving Logs	152
Viewing and Deleting Saved Logs	152

	Using the Log Viewer Tool	153
Appendix B	Avid ISIS 7500 Switch Blade Agent	155
	Understanding the Switch Agent Interface	155
	System Tab	157
	Statistics Tab	159
	Tools Tab	159
	Logging Tab	160
	Advanced Tab	160
	Viewing System Information for Individual Chassis Switches	161
	Setting Chassis Time	161
	Resetting an Avid ISIS Engine to Factory Defaults	162
	Switch Infrastructure Diagnostics	163
	Stacking	163
	Performance	164
	Counters	165
	Connectivity	165
	Hardware	166
	Advanced	167
	Environment	167
	Running Switch Infrastructure Diagnostics	167
	Switch Diagnostics Results	168
	Switch Blade Logging	169
	Using Agent Logging	169
	Viewing Agent Event Logs	169
	Clearing Agent Event Logs	169
Appendix C	Avid ISIS SNMP MIB Reference	171
Appendix D	Avid ISIS E-mail Notification List	173
Appendix E	ISIS 5500 Media Drive LED Functions	180
	Index	182

Using This Guide

The Avid® ISIS® media network provides a high-performance distributed file system that contains high-capacity shared media storage for workgroups of connected Avid editing workstations. This user's guide describes how to connect your client system to the media network, mount workspaces, and configure your system for best performance.

Unless noted otherwise, the material in this document applies to the Windows®, Mac OS® X, and Linux operating systems. The majority of screen shots in this document were captured on a Windows system, but the information applies to all operating systems. Where differences exist, information on the differences is provided.



The documentation describes the features and hardware of all models. Therefore, your system might not contain certain features and hardware that are covered in the documentation.

Who Should Use This Guide

This user's guide is intended for users who need to access workspaces on the Avid ISIS media network. You should have a basic understanding of how to use and manage the Windows operating system or the Mac OS X systems, and you should be familiar with basic workgroup and network concepts.

Symbols and Conventions

Avid documentation uses the following symbols and conventions:

Symbol or Convention	Meaning or Action
	A note provides important related information, reminders, recommendations, and strong suggestions.
	A caution means that a specific action you take could cause harm to your computer or cause you to lose data.
	A warning describes an action that could cause you physical harm. Follow the guidelines in this document or on the unit itself when handling electrical equipment.
>	This symbol indicates menu commands (and subcommands) in the order you select them. For example, File > Import means to open the File menu and then select the Import command.
▶	This symbol indicates a single-step procedure. Multiple arrows in a list indicate that you perform one of the actions listed.
(Windows), (Macintosh), or (Linux)	This text indicates that the information applies only to the specified operating system, either Windows Macintosh OS X or Linux.
Bold font	Bold font is primarily used in task instructions to identify user interface items and keyboard sequences.

Symbol or Convention	Meaning or Action
<i>Italic font</i>	Italic font is used to emphasize certain words and to indicate variables.
Courier Bold font	Courier Bold font identifies text that you type.
Ctrl+key or mouse action	Press and hold the first key while you press the last key or perform the mouse action. For example, Command+Option+C or Ctrl+drag.

If You Need Help

If you are having trouble using your Avid product:

1. Retry the action, carefully following the instructions given for that task in this guide. It is especially important to check each step of your workflow.
2. Check the latest information that might have become available after the documentation was published.
New information would be found in the ReadMe file supplied on your Avid software kit located on the installation USB. Documentation is available as a PDF in the software kit and through the user interface.
Always check online for the most up-to-date release notes or ReadMe because the online version is updated whenever new information becomes available. To view the online versions, visit the Knowledge Base at www.avid.com/US/support.
3. Check the documentation that came with your Avid application or your hardware for maintenance or hardware-related issues.
4. Visit the online Knowledge Base at www.avid.com/US/support. Online services are available 24 hours per day, 7 days per week. Search this online Knowledge Base to find answers, to view error messages, to access troubleshooting tips, to download updates, and to read or join online message-board discussions.

Accessing the Online Documentation

The Avid ISIS online documentation contains all the product documentation in PDF format. You can access the documentation in the top-level AvidISISDocumentation folder on the Avid ISIS installer software kit.



The documentation describes the features and hardware of all models. Therefore, your system might not contain certain features and hardware that are covered in the documentation.

To access the online documentation from the software installer kit:

1. Insert the Avid ISIS installer USB into the USB port.
2. Navigate to the `[drive]:\AvidISISDocumentation` folder, and double-click the PDF file for the document you want to view.

Avid Training Services

Avid makes lifelong learning, career advancement, and personal development easy and convenient. Avid understands that the knowledge you need to differentiate yourself is always changing, and Avid continually updates course content and offers new training delivery methods that accommodate your pressured and competitive work environment.

For information on courses/schedules, training centers, certifications, courseware, and books, please visit www.avid.com/support and follow the Training links, or call Avid Sales at 800-949-AVID (800-949-2843).

1 Working with the Avid ISIS Management Console

The Avid ISIS Management Console allows you to access administration functions from any system that has an Ethernet connection to the System Director, as well as from the System Director itself.



Performing administrative functions on more than one Administration site at the same time can cause unexpected results.

When you access the Avid ISIS Management Console, the Login page opens, and the site prompts you to supply a user name and password to log in. If you type the wrong password, an error message appears and the Login dialog box reappears.



When you first install the Avid ISIS software, the login password is blank by default. To set a password for the administrator, see “Changing the Administrator Password” on page 29.

Standard ISIS client users can log in to the Management Console, but they will have limited access to the Management Console interface. They can also view certain information about the network through the Client Manager. For more information about the Client Manager, see the Avid ISIS Client Manager Help. The *Avid ISIS Client Guide* is also included in the AvidISISDocumentation folder in the software kit.

ISIS Nomenclature Used in this Guide

Throughout this guide, any information for the ISIS | 7500 also applies to the ISIS 7000; likewise for the ISIS | 5500 (applies to ISIS 5000), and ISIS | 2500 (applies to ISIS 2000).

Before Performing Administrative Functions

It is critical that clients unmount Workspaces when you do the following:

- Stop and restart the System Director (unmount all Workspaces)
- Change users' or user groups' access (unmount only the affected Workspaces)
- Rename or delete Workspaces (unmount only the affected Workspaces)



If a client is using a Workspace when the ISIS system is taken offline, the connection to the Workspace is broken and data might be lost.

Opening the Management Console

The Avid ISIS Management Console runs within a web browser window. The following web browsers have been qualified for use with the Management Console:

Microsoft Windows

- Microsoft Internet Explorer
- Mozilla Firefox®
- Google® Chrome™

Apple Macintosh

- Safari
- Mozilla Firefox
- Google Chrome

Red Hat Linux

- Mozilla Firefox

To open the Management Console as Administrator:

1. Open your web browser.
2. In the address bar of your browser, type one of the following:

ISIS Model	Option	Enter
ISIS 7500	Name	https://[System Director host name]:5015
	IP Address	https:// [System Director IP address] :5015
ISIS 5500	Name	http:// [System Director host name]
	IP Address	http:// [System Director IP address]
ISIS 2500	Name	http:// [System Director host name]
	IP Address	http:// [System Director IP address]

The active System Director host name is one of the following:

- The System Director Windows host name.
- A host name which has been assigned to the active System Director on your network DNS server(s).

Check with your network administrator if you are unsure of which System Director name to use.

When you enter the ISIS | 7500 System Director address, if any site certification warnings open, click Yes to accept the certificate. If you are not sure about the security requirements of your shared storage network, see your network administrator.

The Login dialog box for the ISIS Management Console opens. The “Username” field is automatically populated with the Administrator user name.

3. Type your password.

For information on changing the administrative password, see [“Changing the Administrator Password” on page 29](#).

4. Click Login (arrow icon), or press Enter.

The Avid ISIS Home page opens.

To log out of the ISIS Management Console:

- Click Logout in the upper right corner of the screen.

Using the Management Console Interface

The ISIS Management Console, which you can access on the System Director or on any Ethernet-attached client, has a user interface where controls are grouped by function and are displayed by clicking the appropriate icons.

To use the ISIS Management Console, you must have Adobe® Flash® Player installed on your system.



The following illustrations are from the ISIS / 7500 Management Console. They might include features not available in the ISIS / 5500 and ISIS / 2500. Non-Administrator users will see a subset of the tools available to Administrators, depending on access privileges.



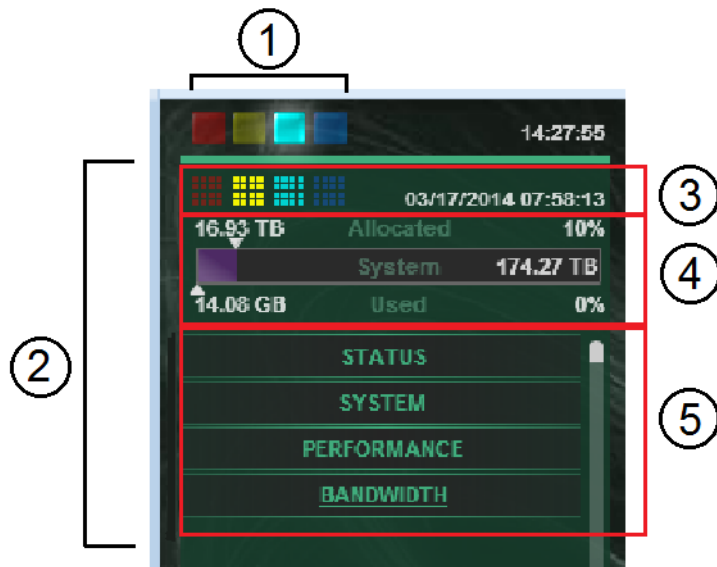
- 1 System Status Console — Provides a snapshot view of several aspects of the Avid ISIS system. See [“System Status Console” on page 17](#).
- 2 Navigation toolbar — Access Management Console tools and bread crumb navigation. See [“Navigation Toolbar” on page 20](#).
- 3 Main tools panel — Click to go to the respective tool pages. See [“Main Tools Panel” on page 21](#).
- 4 Help link — provides links to various ISIS online documents. See [“Main Tools Panel” on page 21](#).
- 5 Logout link — Ends the Management Console session and logs the user out of the system. See [“Opening the Management Console” on page 15](#).

System Status Console

The System Status Console, located on the left side of the Avid ISIS Management Console, contains several components that give you a snapshot view of the Avid ISIS system. These allow you to access additional information about your system and to perform certain administrative tasks, such as monitoring and logging.



Administrators can configure whether or not the System Status Console is visible on the login screen of the Management Console. However, even if it is visible, you must log in to follow links from the tool bar screens (such as the log files).



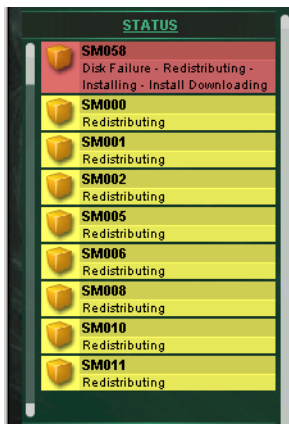
- 1 Current system status panel — LEDs for errors, warnings, info, and upgrade statuses will be lit to indicate the presence of system events. Click a color to open the Status panel. See [“System Status Console Panels”](#) on page 18.
- 2 Status retrieval panel — The Management Console periodically retrieves system status information. The panel displays the results and the time stamp of the retrieval operation.
- 3 System Status History panel — Displays the system events that have occurred since the System Director was started, along with the date and time of the first logged event. Clicking this panel opens the System Status History tool. For more information, see [“System Status History Page”](#) on page 122.
- 4 Storage capacity panel — displays the total capacity of all bound Storage Managers, capacity allocated to Workspaces, and the amount of capacity used by data.
- 5 System Status Console panels — click the panel headings to display the system information panel. For more information, see [“System Status Console Panels”](#) on page 18.

System Status Console Panels

The System Status Console contains several panels that provide information about different areas of Avid ISIS operation. Expand and collapse a panel by clicking the panel title.

Panel	Description
-------	-------------

Status Console Panel	Provides a quick summary of the System Director status. If an event in the system log triggers a status to appear, a link is provided to the System Logs tool. For more information, see “Using the System Logs Page” on page 119
----------------------	---



System Console Panel	Provides a summary of hardware, software, and networking information.
----------------------	---



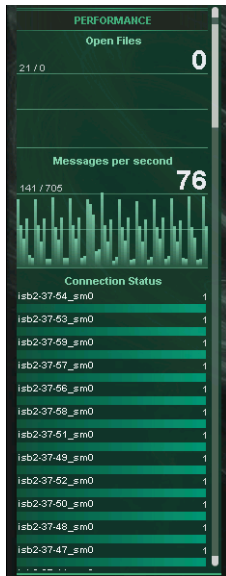
An error message is displayed in the Status panel if the system drives (C: and D:) become too full (defined as less than 6 GB free space on drive C:, or less than 16 GB on drive D:).

A warning message is displayed when the C: drive has less than 11 GB, or the D: drive has less than 26 GB.

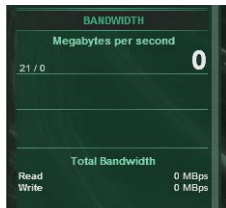
If the C: or D: drives become too full, the system might not be able to save metadata, and you might not be able to upgrade the ISIS software.

If these events or warnings occur, look on the C: and D: drives on the System Director and delete any old ISIS installation kits, and anything in the /temp folder. You can also delete copies of the PartitionDump.bin file that are more than one month old, and any IndexServer.dmp files.

Panel	Description
Performance Console Panel	Provides a summary of the number of messages per second, number of open files, and the names of clients connected to the system.



Bandwidth Console Panel	Displays “Megabytes per second,” information on total and per-client bandwidth.
-------------------------	---



Navigation Toolbar

The navigation toolbar provides several items to help you navigate through the Management Console interface.



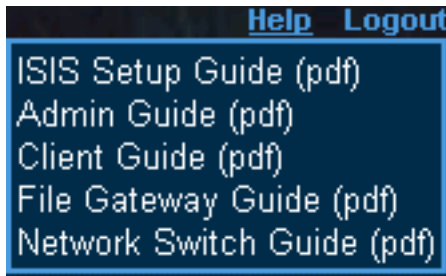
- 1 Home link—You can click this link from any page to return to the Management Console Home screen
- 2 Current tool heading—Indicates the tool you are currently using
- 3 Related links section—Displays links to other Management Console tools relevant to the one you are currently using

Accessing Help

The Help menu, located in the upper right-hand corner of the Management Console window, provides links to the complete set of Avid ISIS online PDF documents.



PDF documents can open in an external application or browser, depending on your configuration. An Administration Guide HTML Help is only available from the System Director Control Panel and requires Internet Explorer. The Help does not work properly in other browsers.

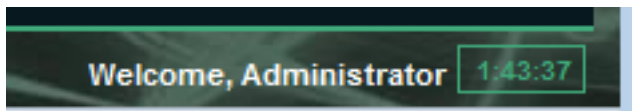


To access the Help menu:

1. Move the mouse cursor over the Help menu text.
The Help pop-up menu opens.
2. (Option) Click the Help menu text to open the Avid ISIS online document.

Session Counter

The user session will time out automatically after two hours of inactivity, after which you must log in again to continue working. The session counter, located in the lower right corner of the Management Console, displays the time remaining in the user session.



The counter is automatically reset to two hours when you click a link or perform an action such as adding or deleting a Workspace. You can also reset the counter manually by clicking it.

If you enable Auto refresh on a tool screen you will not automatically be logged out after two hours, as long as you stay on the page where Auto refresh is enabled, or navigate between tools as described in [“Updating Information” on page 25](#). Clicking Home disables Auto refresh, and the session counter functionality (automatic logout) resumes.

To manually reset the session counter:

- Click the session counter display.
The session timer is reset to two hours.

Main Tools Panel

The ISIS Management Console main panel is divided into the following sections:

- The System section, which contains the following tools:

Tool	Description
Workspaces	View details of, create, delete, duplicate, or change capacity of any Workspace; see “Managing Workspaces” on page 69 for more information.

Tool	Description (Continued)
Users	View details of, create, delete, duplicate, or modify Workspace access of any User; see “Managing Users” on page 90 for more information.
Groups	View details of, create, duplicate, modify Workspace access of, or assign User access to any User Group; see “Managing User Groups” on page 96 for more information.
Devices	View details of, create, delete, or modify descriptions of any device; see “Managing Devices” on page 106 for more information.
Installers	Download installers for Avid ISIS Client Manager, Flash, and other software.
Engines	View details of Engines, reported serial number, status, uptime and more information, see “Managing Storage Managers” on page 33 .
Switch Blades (7500)	View switch IP addresses, Upgrade Switches, or open the switch Agent pages; for more information, see “Managing Storage Managers” on page 33 .
Storage Managers	View details of, bind, or unbind any Storage Manager; for more information, see “Managing Storage Managers” on page 33 .
Storage Groups	View details of, create, delete, or modify Storage Managers of any Storage Group; for more information, see “Managing Storage Groups” on page 61 .

- The Connectivity section, which contains the following tools:

Tool	Description
Connection Status	View or disconnect any connected client; for more information, see “Monitoring System Connection Status” on page 111 .
Bandwidth	View read and write bandwidth of any connected client; for more information, see “Monitoring Client Bandwidth” on page 110 .
Reservations	View and revoke any current bandwidth reservation; for more information, see “Monitoring Reservations” on page 113 .

- The Tools section, which contains the following tools:

Tool	Description
System Status History	View historical system status information; for more information, see “System Status History Page” on page 122 .
Network Utilities	Allows you to retrieve a detailed look at the connected network, or run a ping or traceroute; for more information, see “Network Utilities Page” on page 131 .

- The Logging section, which contains the following tools:

Tool	Description
System Information	Get complete system information: Memory stats, host information, running processes, and Agent statistics, all on one screen; for more information, see “System Information Page” on page 116 .
System Logs	View all system messages, info, warnings, and errors at the application, system, and security levels; for more information, see “Using the System Logs Page” on page 119 .
Administration Logs	View current and archived Management Console logs; for more information, see “Using the Administration Logs” on page 118 .
ISIS Snapshots	Create a snapshot of the ISIS system for viewing or downloading; for more information, see “ISIS Snapshots Page” on page 120 .
Profiler	Create and view profiles of the System Director; for more information, see “ISIS Snapshots Page” on page 120 .

- The Advanced section, which contains the following tools:

Tool	Description
Preferences	Change and save bandwidth, LCT threshold, device creation, disk error threshold, and other preferences; for more information, see “Configuring Management Console Preferences” on page 28 .
External Authentication	Configure external authentication servers; for more information, see “Configuring External Authentication” on page 30 .
Notification Service	Configure email notification on specific system events; for more information, see “Configuring the Notification Service” on page 31 .
Agent Settings	Modify agent configuration options and trace settings; for more information, see “Agent Settings Page” on page 139 .
Administrator Password	Change the Management Console Administrator password; for more information, see “Changing the Administrator Password” on page 29 .

Organizing Display Information

You can customize the Main display panel for any option by moving and hiding columns, and by sorting and filtering information.

Moving Columns

To move a column in the Main display panel:

- Click and drag any column to the position you want, and release the mouse button.
The column appears in the new position, and columns to the right are moved to make room.

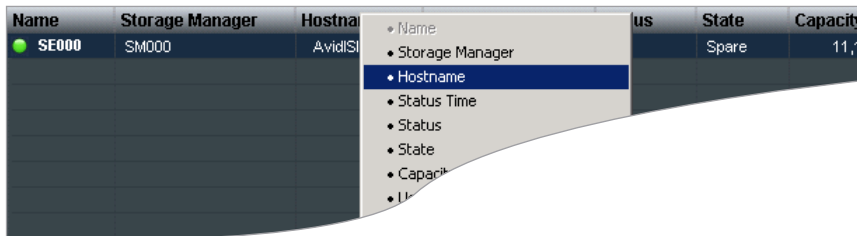
Showing and Hiding Columns

When you open a Management Console tool (for example, the Storage Managers tool), the Main display panel lists items in default columns. Depending on the option selected, there might be other headings available to view. You can select individual or multiple column headings to be displayed or hidden.

To show or hide columns:

- ▶ Select one of the options, right-click in the column heading row and select a heading you want to show or hide.

Displayed column headings are marked by a bullet symbol (•). You cannot hide the first column on the left of the Main display panel (usually the Name column).



Sorting Information

The ISIS Management Console interface allows you to sort information listed in the Main display panel, or in the Details panel. Sorting the information in columns arranges items in either numerical or alphabetical order. You can also perform a multilevel sort of the displayed information.

To sort information:

- ▶ Click the column heading for the column you want to sort.

The information is sorted in ascending order. To reverse the sort order, click the column heading again.

To perform a multilevel sort:

1. Click the column heading for the first column you want to sort.

The items in the column are sorted in ascending order.

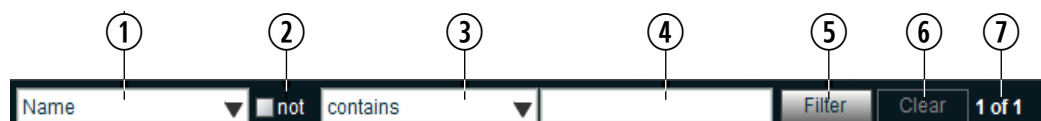
2. Click a second column.

The items in the second column are sorted in ascending order. The items in the first column maintain their sort order, but with a lower priority than the second sort.

3. (Option) Click multiple columns to add levels to the sort. To cancel a multilevel sort, click a column heading that has already been sorted.

Filtering the Display

You can limit the items listed in the Main display panel by setting Filter parameters at the bottom of the Management Console window. Filtering the display allows you to focus on only those items that you want to monitor. You can restore all items to the display by clearing the Filter parameters.



-
- 1 Category menu—Select the category to filter
 - 2 “not” operator—Select to exclude items matching the filter rules from the search results
 - 3 Condition menu—Select the filter condition
 - 4 Search term field—Type the text or value to filter
 - 5 Filter button—Perform the filter operation
 - 6 Clear button—Clear the filter settings
 - 7 Filter results counter—Displays the number of filtered results on the page, and in total
-

You cannot filter the display for the Bandwidth, Connection Status, and Reservation options.

To filter the display:

1. Select a category from the Category menu.

The Category menu lists all of the column headings available for the selected Command menu option.

2. (Option) Select “not” to exclude the items matching the filter rules from the search results.
3. Click the Condition menu and select the filter condition you want to use.
4. In the Filter text box, type the text or value you want to use to filter the display.
5. Click Filter.

The Main display panel updates to display the filtered results. The Filter panel displays the number of filtered items displayed and the total number of items available for display.

To restore all items to the display:

- ▶ Click Clear.

The Main display panel updates to display all items.

Updating Information

You can update onscreen information to reflect recent system changes by clicking Refresh. You can also use Auto refresh to automatically refresh information at timed intervals, and prevent your session from timing out.

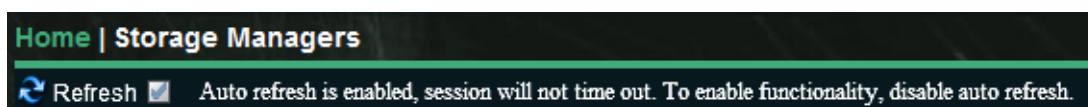


This setting persists between tools, when you navigate between them using the Related Links, but not between browser sessions, and not if you click Home and then back into the tools. In those cases, Auto refresh reverts to the default (disabled) setting.

To enable Auto refresh:

- ▶ Select the check box next to the Refresh.

Auto refresh mode is enabled, and a message is displayed.



While Auto refresh mode is enabled, other functions such as add, delete, and details are not available.

To disable Auto refresh:

- Deselect the check box next to the Refresh.
- Auto refresh mode is disabled, and the confirmation message closes.

Selecting Items

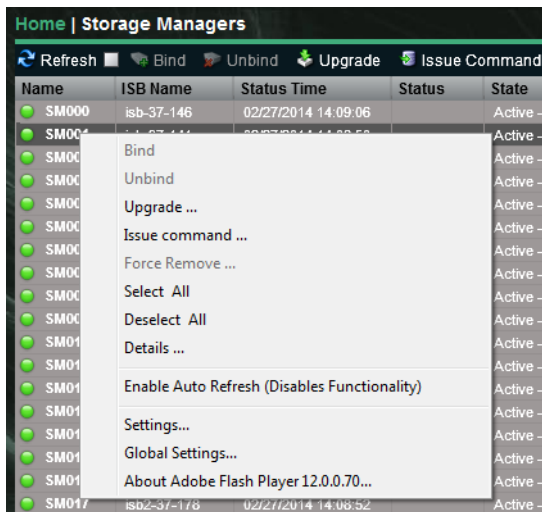
You can select multiple items in most Management Console tool windows. The methods for selecting more than one item in a list are similar to those used in Windows Explorer or the Macintosh Finder.

The following table summarizes the methods for selecting items and performing actions.

Actions	Selection Method
To select an item	Click the item.
To select multiple, non-contiguous items	Ctrl+click each item you want to select.
To select multiple, contiguous items	Click the first item, then Shift+click on the last item.

Using Context Menus to Perform Actions

Most Management Console tool windows offer context menus you can use to perform commands on selected items.

**To access context menus within the Management Console:**

- Right-click (Windows and Linux) or Ctrl+click (Macintosh) selected items.

Entering Text

Follow these guidelines when entering text in Management Console tool text fields:

- Names can be a maximum of 31 ASCII characters in length.
- Workspace names must use Unicode characters and cannot include a space.

- Passwords can be a maximum of 15 ASCII characters in length.
- Do not include a space in the name fields.
- Do not use a period (.) as either the first or last character in the names you create.
- Avoid using the non-permitted characters listed in the following table in the name fields for workspace, group, file, user, device, or storage group names:

Character	Name
^	Circumflex accent
\	Backslash
/	Forward slash
:	Colon
*	Asterisk
?	Question mark
"	Double quotation mark
<	Less-than sign
>	Greater-than sign
	Vertical line
[	Left square bracket
]	Right square bracket
+	Plus sign
=	Equals sign
%	Percent sign
;	Semicolon
,	Comma
@	Commercial At symbol



The System Director does not support viewing regional language characters in the Management Console.

2 Configuring the Management Console

Avid ISIS provides a number of tools to customize the way the Management Console functions and interacts with the network and other Avid products.

Configuring Management Console Preferences

The Preferences tool allows you to set parameters that apply to the basic functionality of the ISIS Management Console.

To configure Management Console Preferences:

1. From the Management Console home page, click the Preferences icon, located in the Advanced section.

The Preferences tool opens.

2. Configure ISIS preferences. The following table summarizes the ISIS Preferences items.

Option	Type	Description
Total System Bandwidth (MB/sec)	<i>text (numeric)</i>	Total reservation bandwidth allowed by the system, in MB/sec. Default value is 1,000 MB/sec. When this value has been reached, ISIS will no longer accept bandwidth reservations from clients.  <i>This value does not represent the actual bandwidth capabilities of the ISIS system. For more information about ISIS bandwidth capabilities, see the Avid ISIS Performance Guide.</i>
Default Bandwidth for Auto Created Devices (MB/sec)	<i>text (numeric)</i>	Reservation bandwidth allowed for devices that are automatically created at connection time. Default value is 0 (zero). Using the default value results in auto-created devices being granted unlimited bandwidth.
Force Manual Device Creation	<i>check box</i>	If enabled, clients which do not have an entry in the Devices list will not be allowed to connect. The Administrator must manually create a device account for every client computer that is expected to connect to the ISIS system. Default value is disabled.
Show status prior to login	<i>check box</i>	When selected, prevents anyone from seeing the Status Console panel on the left side before they log in. Only administrators can change this setting. This setting is disabled by default; users can see the Status Console before logging in.
 The following options should only be altered under the direction of qualified Avid service or support personnel.		
Default LCT Threshold (ms)	<i>text (numeric)</i>	Defines the upper limit of the Long Command Time (LCT) value, above which the Storage Manager will report a Disk Degraded condition to the System Director. Default value is 0 (zero). Using the value of zero sets the LCT threshold to the internal system default of 750ms.

Option	Type	Description (Continued)
Default Hard Disk Error Threshold	<i>text (numeric)</i>	Defines the upper limit for number of hard disk errors before the Storage Manager reports a Disk Failure condition to the System Director. Default value is 0 (zero). Using the value of zero sets the LCT threshold to the internal system default of 25 errors).
Enable failover if standby has more active NICS (7500 and 2500)	<i>check box</i>	When enabled, this causes the Active System Director to failover to the Standby System Director if the network connection fails. Default value is enabled.
Auto Remove Redistribution on Disk Failure (7500)	<i>check box</i>	Default value is enabled. For more information about Auto Remove Redistribution, see “Automatic Redistribution on Disk Failure” on page 83 .
Delete Logging	<i>check box</i>	Logs all deletes performed in the Storage Groups. For more information about delete logging, see “Creating a Log of File Deletions” on page 29 . Default value is disabled.
Auto-Rectify	<i>check box</i>	Automatically reconciles the actual amount of used space and the reported amount of used space on a system. Default value is disabled. Takes effect immediately with no restart required.

3. (Option) To revert all options to the previously saved values, click Refresh.

4. Click Save Preferences to save your changes.

Creating a Log of File Deletions

The delete-logging function is controlled in the Management Console Preferences. When enabled, log files are created and saved in the following location:

D:\Program Files\Avid\ISIS System Director\DeleteLogs

Log file names include name contains the date and time, for example “ISISdeleteLog-07_17_2012_17_59_30_322.csv.” Individual log files are limited to 4 MB in size except where a new log file would have the same name as an existing one. Up to 100 log files are kept then the oldest files are deleted.

You can view the delete log files (.csv) using Microsoft® Excel®. The first field does not display the date until you select the cell and click the text entry box at the top of the spreadsheet.

Each entry in the log file consists of the following fields:

- Date and time of the file delete (19 characters)
- Name of the ISIS user initiating the delete (32 characters)
- Name of the client system the delete was issued from (32 characters)
- Full path of deleted file starting with the workspace name

Changing the Administrator Password

The Management Console Administrator password is blank by default; it is highly recommended that you set an Administrator password when you use the Management Console for the first time.

To change the Administrator password:

1. From the Management Console home page, click the Administrator Password icon, located in the Advanced section.
The Administrator Password tool opens.
2. Type the current Administrator password in the Current Password field (blank by default).
3. Type the new Administrator password in the New Password field.
4. Type the new Administrator password again in the Verify Password field.
5. Click Change.
 - The Administrator Password is changed to the new value.
 - A confirmation message appears in the Results area.

Configuring External Authentication

Users added to the system through the LDAP Sync Tool are automatically configured as remote LDAP users in the ISIS system. When a remote LDAP user logs into the ISIS system, ISIS checks with an external LDAP server to authenticate the user instead of the local ISIS user database. Before remote LDAP users can access the ISIS system, you must configure ISIS to use an external LDAP server for authentication.

For more information on working with LDAP users and groups, see [“Managing LDAP Accounts” on page 99](#).

To configure external Authentication:

1. From the Management Console home page, click the External Authentication icon, located in the Advanced section.
The External Authentication tool opens.
2. Click the Enable check box to select it.
The Domain Name text box becomes active.
3. In the Domain Name text box, enter the domain name of the network which the LDAP server(s) are members of, including subdomains, if applicable.
Use the format *subdomain.domain.top-level-domain*; for example:
`dir.company.com`
4. Click the “Server 0” check box to select it.
The Address text box becomes active.
5. In the Address text box, enter the fully-qualified domain name of the LDAP server.
Use the format *servername.subdomain.domain.top-level-domain*; for example:
`server1.dir.company.com`
6. (Option) Repeat steps 3 – 5 (using the “Server 1” and “Server 2” check boxes) to configure additional backup LDAP servers, if applicable.



All of the LDAP servers must be mirrors, and reside on the same subdomain/domain.

7. When you have finished entering server information, click Submit.
The domain and LDAP server information is added to the ISIS database, and a confirmation message is displayed in the Results area.

Configuring the Notification Service

You can use the Notification Service tool to configure System Director to notify you when problems occur. An error notification service regularly polls the Windows System Event log and, if any errors are logged, sends a concise summary of those errors to one or more email accounts.

The Notification Service tool window is divided into three main sections:

- Configuration – Start and stop the Notification Service, and configure the Notification Service settings.
- Filters – Modify the parameters that define when email notifications are sent to email recipients.
- Contacts – Add and modify email recipients.

Starting, Stopping, and Configuring the Notification Service

The configuration information for the notification service (SMTP information, contacts, and filters) is currently stored in the registry on the System Director. This information is not currently replicated to the Dual System Director server, so you must enter configuration information for notification service on both System Directors.

To configure the Notification Service:

1. From the Management Console home page, click the Notification Service icon, located in the Advanced section.

The Notification Service tool opens.

2. Click the Enable Service check box to toggle between checked and cleared.
 - ▶ If the check box is checked, the Notification Service is enabled.
 - ▶ If the check box is cleared, the Notification Service is disabled.
3. (Option) configure the Notification service settings. The following table summarizes the Notification Service settings.

Option	Type	Description
SMTP Server	<i>text</i>	The IP address or host name of your SMTP server.
SMTP Port	<i>text (numeric)</i>	The port number of your SMTP server. The default value (25) is appropriate in most instances.
Poll Frequency (seconds)	<i>text (numeric)</i>	The frequency (in seconds) with which the error notification service checks for problems.
Return Address	<i>text</i>	The email address of the Avid ISIS administrator or other primary contact for the error notification service.

4. (Option) To test the configuration settings, click Test.

The results of the service test are displayed in the Results area.
5. Click Save.
 - A confirmation message is displayed in the Results area.
 - If you started or stopped the Notification Service, the Service State will change to reflect the new service state.
6. (Option) Click Reset.

The changes for the configuration will be lost.

Configuring Error Notification Parameters

The Filters area of the Notification Service tool window allows you to specify the type of error message that triggers an email notification and to set parameters for each type of error message—Error, Warning, and Information messages.

You can configure the ISIS to send notification emails for one or more error types and what severity level on which to be notified.

For a complete list of Avid ISIS email notifications, see [“Avid ISIS E-mail Notification List” on page 173](#).

To configure error notification parameters:

1. In the Filters section, select or deselect individual notifications by clicking the check boxes corresponding to the error notification.
2. Click Save.

The settings are saved, and a confirmation message is displayed in the Results area.

Configuring Contact Information

You must specify the contact information for all the people you want to receive ISIS notification emails.

To add contacts:

1. In the Contacts section, click New.
Empty User Name and Email fields open.
2. Type a user name into the first text box.
This can be any name you want to assign to the user.
3. Type a valid email address into the second text box.
4. Click Save.
5. Repeat steps 1 – 4 to add more email contacts, if needed.

To remove a contact:

1. Click Delete next to the email contact entry.
The contact is removed from the list.
2. Click Save.

3 Managing Avid ISIS Hardware

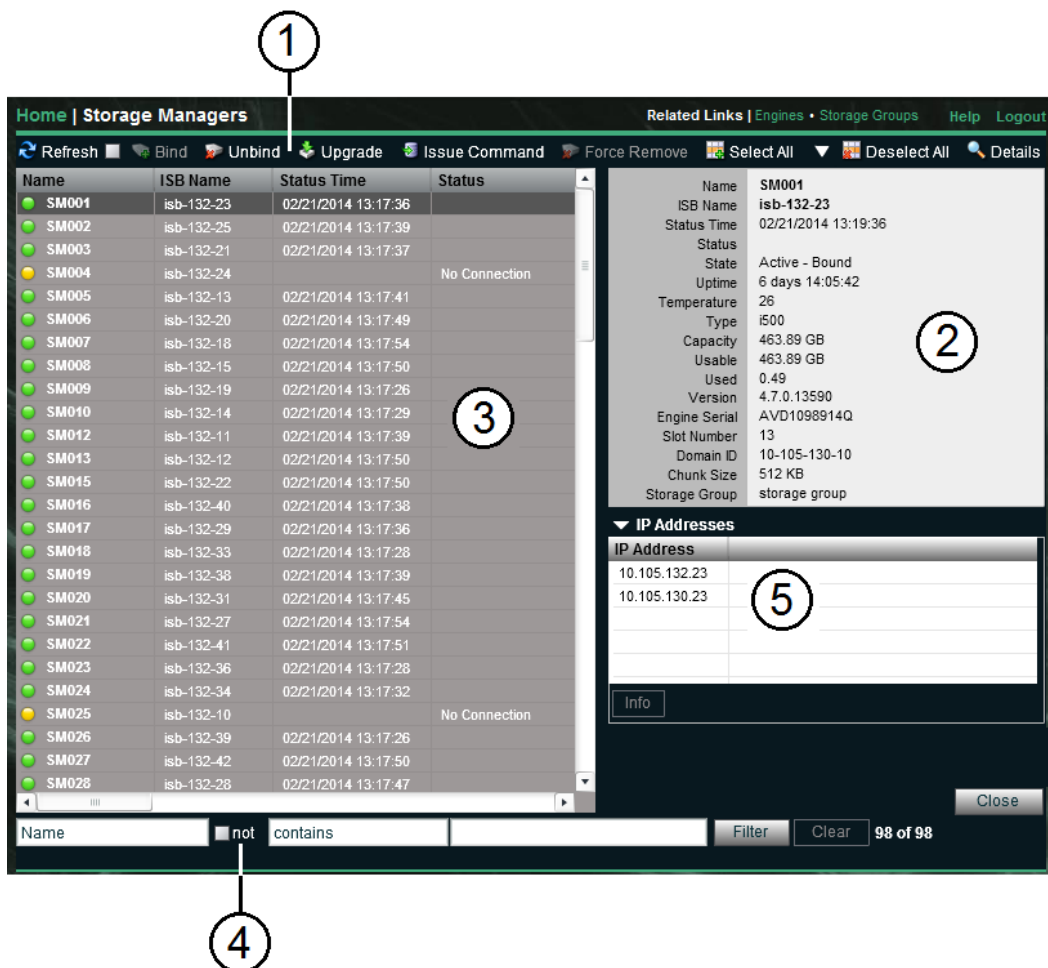
This section describes how to configure and manage your storage hardware. You perform all storage management operations from the Avid ISIS Management Console, which allows you to add, remove, configure, and manage your Storage Managers.

 For an overview of the ISIS Management Console and information about how to start the tool, see “Opening the Management Console” on page 15.

Managing Storage Managers

The Storage Managers tool coordinates and controls the activity of Storage Managers. The Storage Managers tool allows you to bind/unbind Storage Managers and perform maintenance operations.

Before you start building Storage Groups and Workspaces, you must bind each Storage Manager to the ISIS file system to make Storage Managers available for use.



1

2

3

4

5

Name	ISB Name	Status Time	Status
SM001	isb-132-23	02/21/2014 13:17:36	
SM002	isb-132-25	02/21/2014 13:17:39	
SM003	isb-132-21	02/21/2014 13:17:37	
SM004	isb-132-24		No Connection
SM005	isb-132-13	02/21/2014 13:17:41	
SM006	isb-132-20	02/21/2014 13:17:49	
SM007	isb-132-18	02/21/2014 13:17:54	
SM008	isb-132-15	02/21/2014 13:17:50	
SM009	isb-132-19	02/21/2014 13:17:26	
SM010	isb-132-14	02/21/2014 13:17:29	
SM012	isb-132-11	02/21/2014 13:17:39	
SM013	isb-132-12	02/21/2014 13:17:50	
SM015	isb-132-22	02/21/2014 13:17:50	
SM016	isb-132-40	02/21/2014 13:17:38	
SM017	isb-132-29	02/21/2014 13:17:36	
SM018	isb-132-33	02/21/2014 13:17:28	
SM019	isb-132-38	02/21/2014 13:17:39	
SM020	isb-132-31	02/21/2014 13:17:45	
SM021	isb-132-27	02/21/2014 13:17:54	
SM022	isb-132-41	02/21/2014 13:17:51	
SM023	isb-132-36	02/21/2014 13:17:28	
SM024	isb-132-34	02/21/2014 13:17:32	
SM025	isb-132-10		No Connection
SM026	isb-132-39	02/21/2014 13:17:26	
SM027	isb-132-42	02/21/2014 13:17:50	
SM028	isb-132-28	02/21/2014 13:17:47	

Related Links | Engines • Storage Groups | Help | Logout

Refresh Bind Unbind Upgrade Issue Command Force Remove Select All Deselect All Details

Name SM001
ISB Name isb-132-23
Status Time 02/21/2014 13:19:36
Status Active - Bound
State
Uptime 6 days 14:05:42
Temperature 26
Type i500
Capacity 463.89 GB
Usable 463.89 GB
Used 0.49
Version 4.7.0.13590
Engine Serial AVD1098914Q
Slot Number 13
Domain ID 10-105-130-10
Chunk Size 512 KB
Storage Group storage group

IP Addresses

IP Address
10.105.132.23
10.105.130.23

Info

Name not contains Filter Clear 98 of 98

Close

1	Action button toolbar — Perform actions on selected Storage Managers
2	Details panel—Detailed information on the selected Storage Managers; see “Viewing Storage Manager Details” on page 35
3	Storage Managers list — Lists all configured Storage Managers and related information; see “Storage Manager Column List” on page 34
4	Filter panel — Filter the Storage Managers list display based on conditions you configure; see “Filtering the Display” on page 24
5	IP addresses list — Displays the IP addresses of the selected Storage Manager

Storage Manager Column List

The following table summarizes the basic information available when you first open the Storage Manager list. Some columns are hidden by default (see [“Showing and Hiding Columns” on page 24](#)).

Heading	Description
Name	Displays the system-created name of each Storage Manager connected to the system
ISB Name (ISIS 7500)	Displays the name of the ISB in the ISIS 7500 Engine
Hostname (ISIS 5500 and ISIS 2500)	Displays the host name of the Storage Manager (System Director or Engine)
Status Time	Lists the last time the System Director logged the Storage Manager’s status
Status	Displays any change in the working status logged by the System Director (for a description of status messages, see “Storage Manager Status” on page 36)
State	Displays the Storage Manager state (Bound/Unbound)
Uptime	Displays the amount of time Storage Manager service has been running (days:hours:min:sec)
Temperature (ISIS 7500)	Displays the temperature of each ISB in the ISIS 7500 Engine
Type	Displays the Storage Manager type (ISIS 7500 - ISB size, ISIS 5500 - ISIS Engine, ISIS 2000 - Nearline Engine)
Capacity	Displays the total capacity of all Storage Managers controlled by the selected Storage Manager
Usable	Displays the amount of storage space in gigabytes (GB) remaining
Used	Displays the amount of used space in gigabytes (GB)
Version	Displays the software version number of each Storage Manager
Engine Serial	Displays the serial number of the Engine
Slot Number (ISIS 7500)	Displays the slot location of the ISB in the Engine, see “Identifying the ISIS 7500 Storage Managers Prior to Removal” on page 41
Domain ID (ISIS 7500)	Displays the domain ID number of the Management Domain (stack) for each Engine (chassis) in which the Storage Manager is part of.  <i>Domain ID numbers are not displayed until the Storage Managers are bound.</i>
Chunk Size	Displays the smallest unit of data that can be written to the shared storage network.

Heading	Description (Continued)
Storage Group	Displays the Storage Group, if any, to which the Storage Manager is allocated.



You can organize the information in the Storage Managers list by showing additional columns or by sorting or filtering displayed items. For more information on modifying the display, see “Organizing Display Information” on page 23.

A color-coded icon precedes the name of each Storage Manager, providing an indication of the status of the component. The following table describes the color coding system used by the ISIS Management Console.

Icon Color	Description
White	Indicates the status of the Storage Manager is Unbound (the Storage Manager is not linked to the ISIS file system)
Green	Indicates the Storage Manager is bound to the file system
Yellow	Indicates one of the following: - a problem with the Storage Manager - the Storage Manager is experiencing degraded performance
Blue (ISIS 7500)	Indicates that an installation or software upgrade is in progress
Red	Indicates a Storage Manager problem, including any of the following: - a hardware error - a failed software installation or upgrade

Viewing Storage Manager Details

The Details panel displays all information for the currently selected Storage Manager. The information displayed is the information as seen by the System Director. Some of the information is embedded in the Storage Manager, and other information is assigned to the Storage Manager by the Avid ISIS software.

The information displayed in the Details panel is the same as that shown in the Storage Managers tool; see “[Storage Manager Column List](#)” on page 34.

To view detailed information about a Storage Manager:

1. In the Storage Manager list, select a Storage Manager.
2. Do one of the following:
 - ▶ Click Details.
 - ▶ Double-click the Storage Manager name.

The Details panel displays all the information for the selected Storage Manager. For more information, see “[Viewing Storage Manager Details](#)” on page 35.

To close the Details panel:

- ▶ Click Details.

Storage Manager Status

The Status column in the Storage Managers list reports the status of the Storage Managers logged by the System Director. (The Status line in the Details panel reports the same information.) If the Storage Manager maintains a working status, the ISIS Management Console lists no entries in the Status field. When a problem arises, or when the status of the Storage Manager changes, the ISIS Management Console updates the Storage Managers display.

The following table summarizes the Storage Manager status messages, in alphabetical order.

Status	Description
Data conversion mode	A fully populated ISIS 2000 system is running a one-time data conversion redistribution. This mode applies only to ISIS v4.5 on ISIS 2000, and is required to upgrade a fully populated ISIS 2000 from v4.5).
Demonstration mode	A system is configured to run in demonstration mode with limited ability. Demonstration mode runs on non-approved hardware (such as a laptop).
Disk Failure	The hard disk error threshold for a disk has been exceeded and the Storage Manager has taken the disk offline. The default threshold is 25 hard errors. - For the ISIS 7500, a Storage Manager or disk showing this status should be removed from the Storage Group, triggering a redistribution. Once the redistribution is complete, the Storage Manager on the ISIS 7500 can then be removed from the file system, and physically removed from the Engine. - For the ISIS 5500 and ISIS 2500, the disk should be removed, not the entire Storage Manager. The disks should be left physically in the Engine as the disk participates in the redistribution.
Disk full	One or more Storage Managers in a Storage Group has reached its full capacity. Even if some of the Storage Managers still have available space, the Storage Group is considered full as soon as one Storage Manager is filled. As data is written and deleted, some Storage Managers are filled before others. During redistribution, the data is redistributed evenly among the Storage Managers.
Disk Performance Degraded	Disk Performance Degraded: There are two parameters that can trigger this status. - A disk has logged a Long Command Time. The ISIS system periodically clears this log. The Long Command Time counter is also cleared during a reboot. - Once a disk reaches 75% of its hard error threshold, it triggers disk performance degrade. This status is reset only by rebooting the Engine. If an ISIS 7500 Storage Manager is reporting this status, remove the ISB from the Storage Group, triggering a redistribution.
Drive controller error	(ISIS 5500) The drive controller has reported an error.
Foreign disk	A drive with an existing RAID signature has been inserted into a system and cannot be used as a spare or as part of a RAID configuration until the signature is cleared. To clear the foreign configuration, see the <i>Avid ISIS Setup Guide</i> . When you click "Format Foreign Disks" the Status is cleared.
Initializing	The ISIS 5500 and ISIS 2500 RAID set is being initialized. This could take several hours to several days. You can use the Engine while the RAID set is initializing.
Install failed - Phase #	A message displays if the ISIS 7500 ISB fails during the three phases of the upgrade or during the two phases of the ISIS 2500 upgrade.

Status (Continued)	Description (Continued)
Install needed	This message displays if the ISIS 7500 or ISIS 2500 Storage Manager (Engine Controller in ISIS 2500) is not at the same version of the ISIS System Director software. Select all the storage Managers and click Upgrade.
Install needed - No Connection	(ISIS 7500) This a normal one-time message displayed only during the upgrade from v4.0 and earlier to v4.0.1 and later.
Invalid number of drives	The Storage Manager has determined it doesn't have enough drives to run in the bound operating mode. In this mode the Storage Manager only communicates with the System Director, no clients are allowed to connect, and the Storage Manager is not functional in the Storage Group. Once the Administrator has addressed the issue in the Storage Manager, the Storage Manager must be restarted via the Storage Manager agent.
Invalid spare drive	A replacement drive installed to become the new spare is not qualified as an acceptable spare drive for this Engine. Obtain another replacement drive. When a valid replacement drive is installed, it becomes the new spare and the status is cleared.
Memory Error	The Storage Manager runs a memory test when it starts or restarts reports any errors; this status is persistent. Replace the Storage Manager as soon as possible.
Metadata error	(ISIS 7500) The Storage Manager experienced an error loading metadata from the disk or writing new metadata to the disk (if mirrored in the ISIS 7500, the data on the mirrored Storage Manager is still available and no actual data loss occurs); this indicates that the Storage Manager should be replaced. Reboot the Storage Manager with this status. If “Metadata Error” status exists after a reboot, replace the Storage Manager. If the Metadata Error status clears after a reboot, then no further action is required.
Missing spare drive	(ISIS 5500 and ISIS 2500) A rebuild automatically occurs on drive failure by using a spare disk in the Engine. When the spare has been used to replace a failed disk, this warning message is displayed in the Management Console. Obtain a replacement drive for the failed drive. When the replacement drive is installed, it becomes the new spare and the status is cleared. There is one spare drive in each ISIS 5500 Engine and two spare drives in each ISIS 2500 Engine.
Network degraded	The IP interfaces on the Storage Manager have failed or the Storage Manager experiences at least a 10% error rate (usually due to lost packets), indicating a network communication problem. Although the Storage Manager is reporting and detecting the errors, it is usually not the Storage Manager itself that is the problem. Seating issues, slot issues, midplane problems, switch problems, stacking issues, or anything that contributes to bad data getting to the Storage Manager can cause this status. See the tech note “How to troubleshoot Network Degraded” for further details on how to handle this status.
Offline	(ISIS 7500) The Storage Manager has been taken offline. It is good practice to take a Storage Manager offline before reseating or removing it.
Rectifying Files	The Storage Manager is cleaning up deleted files and verifying existing files. This occurs every time the Storage Manager restarts and every 10 days thereafter, and also when manually initiated. Each Storage Manager staggers their process so that they do not run simultaneously.
Redistribution details available	A problem with redistribution occurred. Open the Agent page for the Storage Manager to see the details.

Status (Continued)	Description (Continued)
Repairing Mirrors	(ISIS 7500) The Storage Manager is repairing mirrored blocks with a single point of failure. This Storage Manager has 25 or more blocks that it cannot mirror to another ISB. This can occur due to transient conditions like another ISB rebooting, network problems, or a redistribution in progress. If this condition persists, further troubleshooting is required.
Server Performance Degraded	The Storage Manager chassis needs to be rebooted as soon as possible.
Test Mode	The disks in the Storage Manager are in test mode. This is an Error Insertion function that should only be done by Avid Customer Support.

Binding Storage Managers to the ISIS File System

Before you start building Storage Groups and Workspaces, you must bind each Storage Manager to the ISIS file system to make Storage Managers available for use.

To bind a Storage Manager to the ISIS file system:

1. Click to select the Storage Manager you want to bind.
2. Click Bind.
A Bind Settings dialog appears.
3. Enter the appropriate chunk size for the Storage Manager (for more information, see [“Storage Groups and Chunk Sizes” on page 63](#)).
4. Click OK to bind the Storage Manager.

The selected Storage Manager is added to the ISIS file system, and its state is changed to Active - Bound.

Unbinding Storage Managers from the ISIS File System

Avid strongly recommends that you wait until any redistribution process completes before unbinding Storage Managers. Redistribution can take a long time; use the Redistribution Monitor tool (see [“Monitoring Redistributions” on page 87](#)) to track the progress and estimate the time remaining.



You cannot unbind a Storage Manager that is part of a Storage Group. You must remove the Storage Manager from its Storage Group first so the system can redistribute data before unbinding the Storage Manager from the file system. For more information about removing Storage Managers from a Storage Group, see [“Removing ISIS Storage Managers from Storage Groups” on page 66](#).

Before you can unbind a Storage Manager from the ISIS file system, it must be in the Spare state.

To unbind a Storage Manager from the ISIS file system:

1. Click to select the Storage Manager you want to unbind.
2. Click Unbind.
A confirmation dialog appears.
3. Click Yes to confirm.

The selected Storage Manager is removed from the ISIS file system and its state changes to Unbound.

Clearing Network Degraded Status Messages

You can use the Issue Command button to clear all Network Degraded status messages from the Storage Managers list. Network Degraded status indicates a high number of errors detected by the Storage Manager (see [“Storage Manager Status” on page 36](#)). If correcting the problem does not clear the status messages, use the Issue Command button to clear the messages and reset the error count.



Correct the cause of the Network Degraded status messages before you clear them from the ISIS Management Console.

To clear all Network Degraded messages in the Storage Managers list:

1. Select one or more Storage Managers from the Storage Managers list.

You can use the Shift and Control keys to select multiple items. For more information, see [“Selecting Items” on page 26](#).

2. Click Issue Command.

The Issue Storage Manager(s) Command window opens.

3. Click Clear Network Degraded, and then click Send.

Upgrading Storage Managers

On ISIS | 7500 and ISIS | 2500 systems, you can use the Storage Managers tool to upgrade the Storage Manager software installed in an Engine and connected to the shared storage network.



On ISIS | 7500 systems, you can also use the Engines page to upgrade Storage Managers (Blades) and switches. For more information, see [“Upgrading ISIS | 7500 Engine Components” on page 47](#).

To upgrade a Storage software:

1. Select the Storage Managers you want to upgrade.
2. Click Upgrade.

The Upgrade Storage Managers dialog box opens.

3. Select the upgrade installer from the list in the right column.

The Command text box displays the location of the upgrade installer.



Do not enter any text in the Command or Options fields except under the supervision of qualified Avid support personnel. Doing so can result in system degradation and data loss.

4. Click Upgrade.

The ISIS Management Console installs the necessary upgrade for the selected Storage Manager. You can monitor the progress of the upgrade either in the Details panel of the Storage Manager tool or in the ISIS | 7500 System Monitor tool.

Removing Storage Managers from the ISIS | 7500 Shared Storage Network

You can remove and replace Storage Managers without stopping the System Director or turning off other components of the network. There are two principal reasons for removing Storage Managers from the system:

- The Manager has a high number of unrecoverable errors
- The Manager has failed or has been removed from the system



If you do not have a replacement for a failed or failing Storage Manager, Avid recommends that you physically leave it in the Engine (ISIS / 7500 only), even after it has been removed from the file system. Proper airflow cannot be guaranteed if a Storage Manager slot is left open.

Before you remove an Avid ISIS Storage Manager from the network, you must redistribute the data stored on the Storage Manager to other Storage Managers in the system. The redistribution occurs before you physically remove the Storage Manager, and the process entails moving data to the remaining drives within the Storage Group. Once you redistribute the data, you add a new Storage Manager to the system and then perform a redistribution again to place data onto the new Storage Manager.



If you physically remove a Storage Manager from the shared storage network before redistribution is complete, data loss can occur.



Maintain an unused block of storage equivalent to one Storage Manager within the Storage Group to allow redistribution from a failing Storage Manager to other Storage Managers within the group.

If possible, redistribute data while the drive is experiencing problems but has not yet been removed from the system. This allows the Storage Manager having problems to participate in the redistribution process by offering its data to both clients and to other Storage Managers.



Often the Storage Manager is still functional, but its performance is slightly degraded — for example, the Storage Manager might have an unrecoverable error on one of its disks, or it might have long I/O times.

If the Storage Manager fails, or if it has been removed from the system, you can perform a redistribution from the mirrored or RAID locations associated with the Storage Manager. However, if any other mirrored location experiences a failure while performing a redistribution, the system can lose data.



If the failed Storage Manager was part of an unprotected Workspace, data loss is likely.

Consider the following when planning a redistribution:

- A one-to-one replacement of Storage Managers might leave you with less storage space in the Storage Group than you require. Instead, plan for using more Storage Managers than you need for storage and bandwidth for each Storage Group. This way, you can keep an optimal amount of available storage space allocated to the Storage Group. This allows you to quickly perform redistribution, rather than attempting a redistribution with only one spare Storage Manager.
- In general, the removal of a Storage Manager is quicker than an addition. This is because all of the other Storage Managers in a Storage Group participate in redistribution by moving a copy of any block held by the Manager to another location. The more Storage Managers in the Storage Group, the more the workload is shared. A single Storage Manager addition is slower than a removal because the Storage Manager receiving the data acts as a limiting factor for the redistribution.
- When you add a new Storage Manager to the Avid ISIS file system and then add it to a Storage Group, the system redistributes data from the existing drives in the Storage Group to the new Storage Manager. This redistribution maintains all previously stored data, but the data might not reside on the same Storage Managers.

The following steps list the actions necessary for removing a Storage Manager:

1. Identify the Storage Manager to replace.
2. Remove the Storage Manager from the Storage Group.
3. View the status of the redistribution and wait for redistribution to finish.
4. Unbind the Storage Manager from the Storage Group.
5. Physically remove and replace the Storage Manager.

6. Add the new Storage Manager to the file system.
7. Add the new Storage Manager to a Storage Group.

For more information on the process of redistributing data and how redistribution affects system performance, see [“Redistribution Guidelines” on page 82](#).



Redistributing while adding a Storage Manager takes longer than redistributing while removing an ISB.

Identifying the ISIS | 7500 Storage Managers Prior to Removal

To identify the Storage Manager to be removed and replaced:

1. Locate the failing or failed Storage Manager. For information on Storage Manager status, see [“Storage Manager Status” on page 36](#).
2. Select the Storage Manager, and do one of the following:
 - ▶ Click Details.
 - ▶ Double-click the name of the Storage Manager.

The Details panel opens.

The Details panel lists the Engine Serial number and the Slot Number of the selected Storage Manager. The slot number identifies the Storage Manager to be physically removed.

0	1	2	3
4	5	6	7
8	9	10	11
12	13	14	15

ISIS slot numbering



The slot numbers for Storage Managers begin at zero (0).

Preparing to Remove Storage Managers from the Avid ISIS Engine

After you have identified the Storage Manager you want to remove, remove it from the Storage Group before you physically remove it from the Engine.



You must finish the redistribution before you physically remove the Storage Manager. If you do not wait until the redistribution finishes, shared storage network clients might receive multiple errors.

To physically remove a Storage Manager from your shared storage network:

1. Remove the Storage Manager from its Storage Group. For information on removing Storage Managers, see [“Removing ISIS Storage Managers from Storage Groups” on page 66](#).
2. Open the Workspaces tool by clicking the Workspaces icon in the System section of the Management Console home page.

The Workspaces tool opens.

3. Select the Workspace for the appropriate Storage Group.
4. Monitor the Status column for to update the display.

The Status column displays no status message when the redistribution is complete. Alternatively, because redistribution can take a long time, you can track the progress of the redistribution in the Storage Managers Monitor tool (see [“Monitoring Redistributions” on page 87](#)).



Do not remove the Storage Manager before the redistribution has completed.

5. Unbind the Storage Manager from the ISIS file system; see [“Unbinding Storage Managers from the ISIS File System” on page 38](#).
6. In the Storage Manager list, select the Storage Manager you want to remove and then click Issue Command.
The Issue Storage Manager(s) Command dialog box opens.
7. Select Take Offline, and then click Send.



If you remove an active Storage Manager by mistake, the System Director restores the Storage Manager to the Storage Manager list the next time it polls the shared storage network (usually within 20 seconds).

The system spins down the drives in the selected Storage Manager and changes the status in the Storage Managers list to Offline.

8. Disconnect the Storage Manager from the network, as described in the *Avid ISIS Setup Guide*.

Removing Orphaned Storage Managers

Orphaned Managers are Storage Managers connected to a file system which is not currently in use. This can happen when a Storage Manager is moved from one ISIS environment to another, or when you use the System Director Control Panel to create a new active partition on a system that already includes bound Storage Managers. The “Force Remove” command will remove the file system binding from the Storage Manager and make it available for use in the current file system.

To remove orphaned Storage Managers, you must force-remove them from the system.



Removing Storage Managers causes all data stored on them to be erased. Do not remove disconnected Storage Managers unless you are certain they contain no data you want to save.

To remove orphaned Storage Managers:

1. From the Management Console home page, click the Storage Managers icon, located in the System section.
The Storage Managers tool opens.
2. Select the orphaned Manager you want to force-remove.
3. Click Force Remove.

A message warns you that removing Storage Managers erases all data on the component.

4. Click Yes.

The Force Removal Text Confirmation dialog box opens.

5. Type **Remove** in the text box, and then click Remove.

The orphaned Storage Manager is unbound from the ISIS file system and removed from the Orphaned Managers list.

Initiate Block Rectify

Once you have added Storage Managers to your network and configured them for storage, the Storage Manager periodically checks the status of stored files, cleaning up deleted files and verifying existing files. This process, called “rectifying files,” allows the Storage Managers to communicate with the System Director to monitor the state of its storage and clean up any files that the Storage Managers no longer need to store. Rectifying files occurs randomly and asynchronously during normal system operation to minimize any potential decrease in system performance. The process is indicated for each affected Storage Manager in the Status column in the Storage Manager list.

Storage Managers also rectify files when starting or restarting. When this happens, data stored on the Storage Managers might not be in sync with the data in the file system itself. Also, if a client, such as the asset manager, cannot communicate with the Storage Manager, there might appear to be more data allocated to the Storage Managers than the file system has allocated. To correct this, you can manually send the Storage Manager a command to rectify its files.

To rectify files:

1. Select one or more Storage Managers from the Storage Managers list.

You can use the Shift and Control keys to select multiple items. For more information, see [“Selecting Items” on page 26](#).

2. Click Issue Command.

The Issue Storage Manager(s) Command dialog box opens.

3. Select Initiate Block Rectify, and then click Send.

The system rectifies files on the selected Storage Managers and changes the status in the Storage Managers list to Rectifying Files.

Managing ISIS | 7500 Switch Blades

The Switch Blades tool of the ISIS Management Console allows you to monitor and upgrade all Switch Blades connected to the shared storage network. You can also launch the Agents for the selected Switch Blades to view details and change configuration.

ISIS | 7500 Switch Blades Column List

The following table summarizes the information available in the Switch Blades list.

Heading	Description
In band IP	Displays the internal IP addresses assigned to the CPU on the switch
Status Time	The time at which the current status display was reported
Status	Displays changes in the working status of the switch
Version	Displays the software version number of each switch
Type	Identifies the switch as one of the following: • Integrated (ISS) • Expansion (IXS)

Heading	Description (Continued)
Temp	Lists the last logged temperature of the switch, in degrees Celsius
Chassis Master	Indicates if an ISS or an IXS module is used as a master switch in the Engine
Base IP	The base IP addresses of the switch, which are assigned during system configuration; for more information, see the <i>Avid ISIS Setup Guide</i>
Out of band IP	The IP address of the Switch Blade management port; for more information about the management port, see the <i>Avid ISIS Setup Guide</i>
Engine Serial	Displays the serial number of the Engine

Viewing ISIS | 7500 Switch Blade Details

You can view detailed information on Switch Blades using Avid ISIS Switch Blade Agents, which can be accessed through the Switch Blades tool. For more information about Avid ISIS Switch Blade Agents, see [“Avid ISIS | 7500 Switch Blade Agent” on page 155](#).

To launch Avid ISIS Switch Blade Agents:

1. From the Switch Blades list, select a Switch Blade.
2. Click Show Info.

The Avid ISIS Switch Blade Agent opens.



The default switch Agent page password is se-admin.

Upgrading ISIS | 7500 Switch Blades

You can use the Switch Blades tool to upgrade the software for Switch Blades installed in an Engine and connected to the shared storage network.



You can also use the Engine page to upgrade Switch Blades. For more information, see [“Upgrading ISIS | 7500 Engine Components” on page 47](#).

To upgrade Switch Blades:

1. From the Management Console home page, click the Switch Blades icon, located in the System section.

The Switch Blades tool opens.

2. Select the Switch Blade you want to upgrade.
3. Click Upgrade Switches.

The Upgrade Switch Blades dialog box opens.

4. Select the upgrade installer from the list in the right column.

The Command text box displays the location of the upgrade installer.



Do not enter any text in the Command or Options fields except under the supervision of qualified Avid support personnel. Doing so can result in system degradation and data loss.

5. Click Upgrade.

The ISIS Management Console installs the necessary upgrade for the selected Switch Blade. You can monitor the progress of the upgrade either in the Details panel of the Switch Blades tool or in the Avid ISIS System Monitor tool.

Managing the Engine

The Engines page of the ISIS Management Console allows you to view details and to monitor the status of all Engine connected to the shared storage network, as well as ISIS | 7500 Storage Managers, ISIS | 7500 Integrated switches (ISS), ISIS | 7500 Expansion Integrated switches (IXS), ISIS | 7500 and ISIS | 5500 power blades, and ISIS 7500 | 7000 upgrades.

Engine Column List

The following table summarizes the information available in the Engine list.

Heading	Description
Serial Number	Serial number of the Engine
Status Time	The last time the System Director logged the status of the Engine
Status	Displays changes in the working status of Storage Manager components due to upgrade installation or failure. On the ISIS 7500 it also displays changes in the working status of ISS and IXS modules due to upgrade installation or failure.
Uptime (ISIS 5500)	Displays the length of time that the Storage Manager has been running continuously
Available	Lists the number of available Storage Managers in each Engine
Spare	Lists the number of spare Storage Managers in each Engine
Active	Lists the number of active Storage Managers in each Engine
Storage Blades (ISIS 7500)	Lists the number of Storage Manager components installed in each Engine
Switch Blades (ISIS 7500)	Lists the number of ISS and IXS modules for each Engine
Power Blades (ISIS 7500 and ISIS 5500)	Lists the number of power supply units for each Engine
Free Memory (ISIS 5500 and ISIS 2500)	Displays the amount of memory not in use
Total Memory (ISIS 5500 and ISIS 2500)	Displays the total amount of available memory
Product Serial (ISIS 5500)	Displays the Avid part number for the ISIS 5500 product. The ISIS 5500 5000 has more than one ISIS 5500 Engine configuration.
Product Part Number (ISIS 2500)	Displays the Avid part number for the ISIS 2500 product.

Engine Details

The Details panel displays all information for the currently selected Engines. The panel is divided into three sections:

- Engine Details — displays the same information as in the Engine list
- Switches (ISIS | 7500) — lists basic configuration and status information of all ISS and IXS modules connected to the shared storage network
- Storage Managers — displays information also available in the Storage Managers list

The information displayed is as seen by the System Director. Some of the information is embedded in the Engine, and other information is assigned to the Engine by the Avid ISIS software.

You can sort the information in the Switches and Storage Managers sections of the Details panel by clicking any column heading. For more information on sorting items in columns, see [“Sorting Information” on page 24](#).



You can view more detailed information on Engine components by using the Avid ISIS Agent tool. For more information, see [“Avid ISIS Storage Manager Agent” on page 141](#) and [“Avid ISIS Storage Manager Agent” on page 141](#).

To view information about an Engine:

1. In the Engine list, select an Engine.
2. Do one of the following:
 - ▶ Click Details.
 - ▶ Double-click the Engine name.

The Details panel displays all the information for the selected Engine.

To close the Details panel:

- ▶ Click Details.

Removing Engines from the Engine List

If you need to replace an Engine, you can use the ISIS Management Console to remove the connection history of the inactive or inoperative Engine from the list in the Engines page. Once the Engine is removed from the ISIS file system, you can physically remove it from the network.

For information on removing Engines from the network, see the *Avid ISIS Setup Guide*.

To remove an Engine from the Engine list:

1. In the Engine list, select the Engine to remove.
2. Click Remove Status.

The Engine is removed from the Engine list.



If you remove an active Engine by mistake, the System Director restores the Engine to the Engine list the next time it polls the shared storage network (usually within 20 seconds).

Upgrading ISIS | 7500 Engine Components

On an ISIS | 7500 system, you can use the Engines page to upgrade the software for all Storage Managers and all Switch Blades installed in an Engine and connected to the shared storage network. You can also upgrade individual Storage Managers and switches.



You might lose network connectivity temporarily when you upgrade Switch Blades while the upgrade process reboots the switches.

To upgrade all Storage Managers and switches in an Engine:

1. In the Engine list, select the Engine to upgrade.
2. Do one of the following:
 - ▶ Click Upgrade Blades.
 - ▶ Click Upgrade Switches.

The Upgrade Storage Managers dialog box or the Upgrade Switch Blades dialog box opens.

3. Select the upgrade installer from the list in the right column.

The Command text box displays the location of the upgrade installer.



Do not enter any text in the Command or Options fields except under the supervision of qualified Avid support personnel. Doing so can result in system degradation and data loss.

4. Click Upgrade.

The ISIS Management Console installs the necessary upgrades for all Storage Managers or for all Switch Blades for the selected Engine. You can monitor the progress of the upgrade either in the Details panel of the Engine page or in the Avid ISIS System Monitor tool.

Upgrading Individual ISIS | 7500 Engine Components

You can upgrade individual Storage Managers and Switch Blades in the Engine page. You can also upgrade Storage Managers by using the Storage Managers page and Switch Blades by using the Switch Blades page. For more information on Storage Manager upgrades, see [“Upgrading Storage Managers” on page 39](#). For more information on Switch Blade upgrades, see [“Upgrading ISIS | 7500 Switch Blades” on page 44](#).

To upgrade individual Storage Managers and switches in an Engine:

1. In the Details panel of the Engine page, do one of the following:
 - ▶ Select the switch you want to upgrade.
 - ▶ Select the Storage Manager you want to upgrade.

2. Click Upgrade.

The Upgrade Storage Elements dialog box or the Upgrade Switches dialog box opens.

3. Select the upgrade installer from the list in the right column.

The Command text box displays the location of the upgrade installer.



Do not enter any text in the Command or Options fields except under the supervision of qualified Avid support personnel. Doing so can result in system degradation and data loss.

4. Click Upgrade.

The ISIS Management Console installs the necessary upgrade for the selected Storage Manager or Switch Blade. You can monitor the progress of the upgrade either in the Details panel of the Storage Managers page or in the Avid ISIS System Monitor page.

4 Avid ISIS Control Panels

When you log into the Avid ISIS System Director desktop, there are several tools available to help you access ISIS tools and perform diagnostic and maintenance tasks.

- [ISIS Launch Pad](#) provides buttons for quick access to various ISIS tools.
- [Avid ISIS System Director Control Panel](#) provides low-level, performance-monitoring functions.

ISIS Launch Pad

ISIS Launch Pad provides buttons for quick access to various ISIS tools. The Launch Pad window remains “docked” to the upper right corner of the System Director desktop, but may be collapsed to a smaller size if needed (see “[Minimizing or Closing the ISIS Launch Pad](#)” on page 51).

The image displays three screenshots of the Avid ISIS Launch Pad control panels for different ISIS models: ISIS 7500, ISIS 5500, and ISIS 2500. Each panel is titled 'Avid © ISIS ® Launch Pad' and 'System Director -'. The panels show various status and performance metrics.

ISIS 7500 Panel:

- Status: Running (green dot)
- Check event log (orange dot)
- Reconfiguration not required (green dot)
- Licenses in use: 2 of 331
- Virtual name: PELHWINDEX
- Version: 4.7.0.13415
- Metadata: Loaded (green dot), Status: Validating (green dot), In use: 0.32%
- Save time: Wed Feb 12 15:30:17 2014
- Verify time: Wed Feb 12 15:30:15 2014
- Redundancy: Enabled: No, Mode: Active, Replicate state: N/A, Replicate time: N/A, Path status not available: N/A
- Performance: Messages per second: 44.7, Write bandwidth (MB/s): 0.0, Read bandwidth (MB/s): 0.0, Open files: 0

ISIS 5500 Panel:

- Status: Running (green dot)
- No warning events logged (green dot)
- Reconfiguration not required (green dot)
- Licenses in use: 0 of 90
- Virtual name: AvidISIS
- Version: 4.7.0.13555
- Metadata: Loaded (green dot), Status: N/A, In use: 0.04%
- Save time: Wed Feb 12 14:53:08 2014
- Verify time: Wed Feb 12 14:53:00 2014
- Redundancy: Enabled: No, Mode: Active, Replicate state: N/A, Replicate time: N/A, Path status not available: N/A
- Performance: Messages per second: 37.3, Write bandwidth (MB/s): 0.0, Read bandwidth (MB/s): 0.0, Open files: 0

ISIS 2500 Panel:

- Status: Running (green dot)
- Check event log (orange dot)
- Reconfiguration not required (green dot)
- Licenses in use: 0 of 200
- Virtual name: ISIS2000UI1
- Version: 4.7.0.0
- Metadata: Loaded (green dot), Status: N/A, In use: 0.01%
- Save time: Wed Feb 12 15:24:51 2014
- Verify time: Wed Feb 12 15:24:44 2014
- Redundancy: Enabled: No, Mode: Active, Replicate state: N/A, Replicate time: N/A, Path status not available: N/A
- Performance: Messages per second: 39.0, Write bandwidth (MB/s): 0.0, Read bandwidth (MB/s): 0.0, Open files: 0

Storage Manager Panel (bottom):

- Status: Running (green dot)
- Fan status (green dot)
- System drive status (green dot)
- Power supply status (green dot)
- Version: 4.7.0.13555

The following information is displayed in the Launch Pad for all ISIS models:

- Status Data:
 - Whether the System Director is running
 - The presence or absence of warning events
 - Whether reconfiguration is required
 - The number of client licenses in use
 - The virtual name of the System Director
 - The version number of the installed software on the System Director
- Metadata:
 - Whether the metadata was successfully loaded by the System Director
 - Metadata status
 - Percentage of allocated memory in use
 - Date and time the metadata was last saved
 - Date and time the metadata was last verified
- Redundancy:
 - Whether redundancy is enabled between dual System Directors
 - Redundancy mode of the current System Director (Active or Standby)
 - Replication state of the System Directors
 - Status of the failover network ports
- Performance:
 - Number of messages transmitted per second
 - Total Write bandwidth in Mb/s
 - Total Read bandwidth in Mb/s
 - Total number of open files in all Workspaces

On the ISIS | 5500, the following additional information for the Storage Manager is displayed:

- Status (running or not)
- Fan status
- System drive status
- Power supply status
- Software version number (ideally, same as the System Director version)

Opening ISIS Launch Pad

ISIS Launch Pad starts with Windows on the System Director and usually remains on the desktop at all times. If it was shut down, you can restart the ISIS Launch Pad from the System Director Windows Start Menu.

To open ISIS Launch Pad on the ISIS | 7500 and ISIS | 2500:

- ▶ Click Start > All Programs > Avid > ISIS System Director > ISIS Launch Pad.

To open ISIS Launch Pad on the ISIS | 5500:

- ▶ Click Start > All Programs > Avid > ISIS Storage Manager > ISIS Launch Pad.

Minimizing or Closing the ISIS Launch Pad

The ISIS Launch Pad window remains “pinned” to the upper right corner of the System Director desktop, but may be collapsed to a smaller size if needed.

To minimize the ISIS Launch Pad:



- ▶ Right-click the Avid ISIS Launch Pad icon on the right side of the Windows Taskbar and select Minimize.

To restore the ISIS Launch Pad:



- ▶ Right-click the Avid ISIS Launch Pad icon on the right side of the Windows Taskbar and select Restore.

To quit the ISIS Launch Pad:



- ▶ Right-click the Avid ISIS Launch Pad icon on the right side of the Windows Taskbar and select Quit.

ISIS Launch Pad Buttons

The following table describes the ISIS Launch Pad buttons. You can also hold the cursor over the button and get a tool tip on the button function.

Button	Function
System Director	
	Starts the System Director. The button is blue when the System Director is stopped. The button is gray when the System Director is running.
	Stops the System Director. The button is blue when the System Director is running. The button is gray when the System Director is stopped.
	Opens the Avid ISIS Management Console in a web browser window (the default browser is Microsoft Internet Explorer). For more information about using the Management Console, see “Opening the Management Console” on page 15 .
	Opens the Avid ISIS System Director Control Panel. For more information, see “Avid ISIS System Director Control Panel” on page 52 .
	Opens the System Director Memory Log Viewer tool. For more information, see “Using the ISIS System Director Memory Log Viewer” on page 56 .
	Opens the Avid ISIS Profiler. Gathers system and version information on the System Director, System Manager, or client. This tool detects the system if is being run on and selects the components automatically. For more information, see “Profiler Page” on page 122 .
Storage Manager (ISIS 5500)	
	Starts the Storage Manager. The button is blue when the Storage Manager is stopped. The button is gray when the Storage Manager is running.

Button	Function (Continued)
	Stops the Storage Manager. The button is blue when the Storage Manager is running. The button is gray when the Storage Manager is stopped.
	Opens the Agent Management page. For more information, see “Opening the Avid ISIS Storage Manager Agent” on page 141 .
	Opens the Network Configuration Tool. This tool is used to set the IP addresses for the network ports on the ISIS 5500 System Director. For more information, see the <i>Avid ISIS 5500 Setup Guide</i> .
	Opens the Storage Manager Memory Log Viewer. For more information, see “Using Storage Manager Memory Log Viewer” on page 52 .
	Opens the Avid ISIS Profiler. Gathers system and version information on the System Director, System Manager, or client. This tool detects the system if it is being run on and selects the components automatically. For more information, see “Profiler Page” on page 122 .

Using Storage Manager Memory Log Viewer

The Storage Manager Memory Log Viewer is a valuable tool that allows you to view the Storage Manager log as it is buffered in memory. This log provides detailed status information that is especially useful to Avid Customer Support personnel for monitoring Storage Manager status during prolonged operations.

To open the Storage Manager Memory Log Viewer:

- Do one of the following:



- In the Storage Manager section of the ISIS Launch Pad, click Storage Manager Memory Log Viewer icon.
- From the System Director desktop, click Start > Programs > Avid > ISIS Storage Manager > Memory Log Viewer
- From the Storage Manager Agent page, click Console viewer in the Tools section (see [“Using the Log Viewer Tool” on page 153](#)).

Avid ISIS System Director Control Panel

The Avid ISIS System Director Control Panel provides low-level performance monitoring functions. Using the Control Panel, you can view the following:

- The current status of connected clients, including name, type, ID number, and active or inactive status
- The status of communications between the System Director and the clients
- Information on the metadata maintained by the System Director

The System Director Control Panel is used to start, stop, and monitor the Avid ISIS System Director, the application running on the System Director server that manages the overall operation of the network. You can also use the Control Panel to configure general or Dual System Director parameters, and to set some administrative options.

Opening the System Director Control Panel

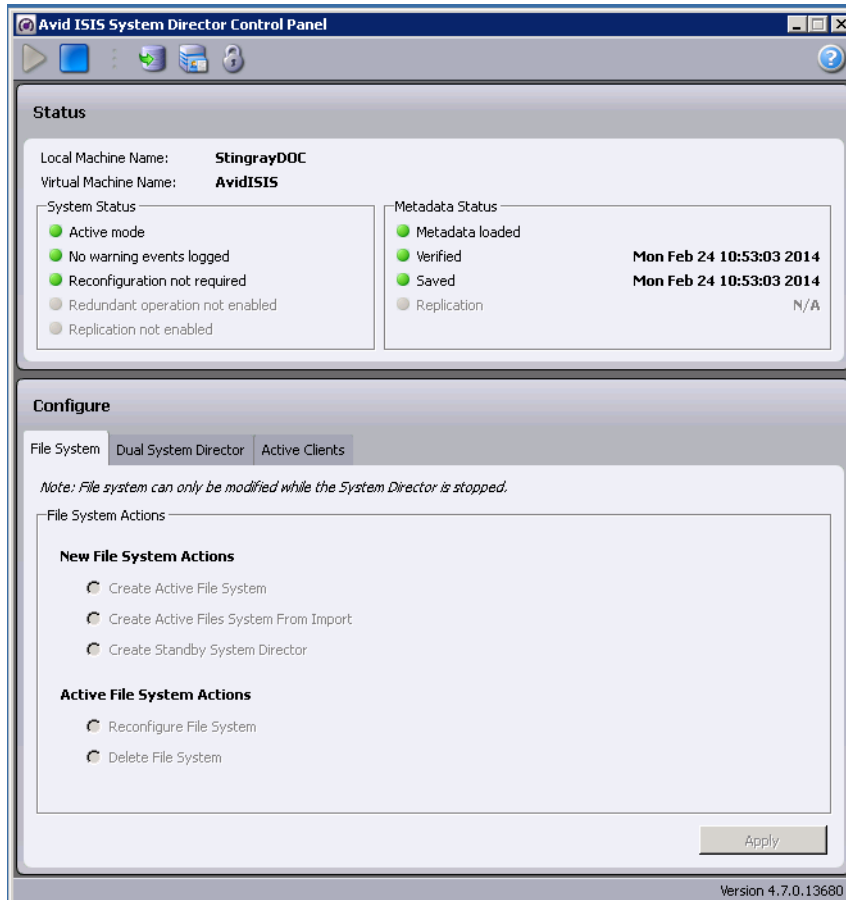
The System Director Control Panel is a Windows application that can be accessed from the Windows Start menu and from the ISIS Launch Pad.

To open the Control Panel, do one of the following:



- ▶ In the ISIS Launch Pad, click ISIS Control Panel icon.
- ▶ From the System Director desktop, select Start > Programs > Avid > ISIS System Director > Control Panel.

The System Director Control Panel opens.



The buttons on the System Director control panel do the following:

-   —Start and stop the System Director windows service
-  —Dump metadata
-  —Change the virtual server name for the System Director
-  —Reset the ISIS password

The following table summarizes the functions available in the Control Panel.

Panel	Tab	Function
Status	(NA)	Displays the local and virtual machine names and a summary of the system and metadata status

Panel	Tab	Function
Configure	File System	This panel is active only when the System Director is stopped. Allows you to: • Create a new active file system on the System Director • Create a new active file system using information imported from another System Director • Create a Standby System Director in a Dual System Director configuration • Reconfigure the existing file system • Delete the file system
Configure	Dual System Director	This panel allows you to configure a Dual System Director configuration, specifying: • Virtual and local addresses • Local and remote machine routing parameters
	Active Clients	The Active Clients tab displays the identity of the Avid ISIS clients known to the System Director, and all active Storage managers. • Click Refresh to refresh the display. • Click Disconnect to disconnect the selected clients.

Starting and Stopping the System Director Service

The System Director software runs as a Windows service that starts automatically whenever the System Director is online. However, various maintenance and administration functions require that you shut down the System Director engine and then restart it.

Maintaining metadata integrity is very important to ensure you do not lose any data files. Avid recommends you use the following procedure prior to System Director engine shutdown to avoid problems with metadata integrity.



In a Dual System Director configuration, Avid recommends that you shut down the standby System Director before shutting down the active System Director. Otherwise, the active System Director fails over to the standby System Director as the active System Director shuts down.



To prevent errors, make sure that clients unmount all Workspaces before you stop the System Director.

To stop the System Director service:

1. Do one of the following:



- ▶ In the ISIS Launch Pad, click Stop System Director.
- ▶ From the ISIS Control Panel, click Stop System Director.

A dialog box opens, prompting you to confirm that you really want to stop the System Director.

2. Click OK.

The System Director Shutdown dialog box opens stating that it is saving multiple copies of the metadata.

Wait for the process to finish and for the dialog box to close. When the System Director has shut down, the System Director Status tab lists the System Director status as “Not running.”

3. (Option) If you are upgrading or modifying the system, make sure the System Director software has successfully written a local copy of the metadata file:
 - a. Open the folder D:\Program Files\Avid\ISIS System Director
 - b. Make sure the files Partition0, Partition1, and PartitionDump.bin exist and have the date and time of when you stopped the System Director. If they do not, call Avid Customer Support.



Pay special attention to the date and time of the Partitiondump.bin file before importing it to recreate a file system. If the PartitionDump.bin file is more than a few hours old, it could cause loss of data or data corruption. Call Avid Customer Support before importing this file to recreate the file system.

- c. Copy (not move) these files to a temporary folder to be used in case there is a problem with the upgrade.

To start or restart the System Director service, do one of the following:



- ▶ In the ISIS Launch Pad, click Start System Director.
- ▶ From the System Director control panel, click Start System Director.

Changing the System Director Virtual Name

The System Director virtual name is the name that is used for the Shared Storage network and appears in the System Director list in the Avid ISIS Client Manager application. The System Director virtual name is set to the Windows computer name by default, but you can change it to a different value.



The System Director virtual name is used only within the Shared Storage network. It has no effect on Windows networking.

To change the virtual System Director name:



1. In the Control Panel toolbar, click Change Virtual System Director Name.

The Change Virtual System Director Name dialog box opens.

2. Type a name for the System Director in the Virtual System Director Name text box.

In a Dual System Director configuration, you must specify the same virtual System Director name for both System Directors.

The naming conventions are the same for the System Director virtual name as they are for Windows network computer names:

- No more than 31 characters in length
- Cannot use the following characters: " \ / [] : | < > + = ; , ?
- Cannot use ASCII control characters in range 0x00 through 0x1F

3. Click OK.

Monitoring System Director Status

The System Director Status panel provides status displays that provide a summary of your network and controls that allow you to start and stop the System Director, and reset the event log.

System Director Status Indicators

When the shared storage network is functioning normally, a green indicator is displayed with the following messages:

- Active Mode
- No warning events logged
- Reconfiguration not required
- Single System Director — Redundant operation not Enabled; Dual System Directors — Both paths are up
- Single System Director — Replication not Enabled; Dual System Directors — Replicated



If your network does not use a Dual System Director configuration, a gray indicator is displayed next to the message, “Redundant operation is not enabled.”

If the indicator is yellow or red, the message changes. Use the following information to correct the problem:

- System Director is not running — start the System Director by clicking Start System Director.
- Check event log — logged significant events related to the System Director are also logged in the Logging tab of the ISIS Management Console. For information on how to extract data in the system logs, see [“System and Administration Log Pages” on page 118](#).
- The following error messages indicate metadata replication status:
 - Replication failed — Indicates that there was an error replicating the metadata to or from a standby System Director.
 - Replication unknown — Indicates that the current replication status has not been determined.
 - Replication status not available — Indicates that the status is unknown. Most likely, the System Director is not running.

Using the ISIS System Director Memory Log Viewer

The System Director Memory Log Viewer allows you to view the System Director log as it is buffered in memory. This log provides detailed status information that is especially useful to Avid Customer Support personnel for monitoring system status during prolonged operations.

To open the System Director Memory Log Viewer:

- ▶ Do one of the following:
 - Click the Memory Log Viewer icon under System Director on the Launch Pad
 - From the System Director desktop, click Start > Programs > Avid > ISIS System Director > Memory Log Viewer

Working with File System Operations

The File System tab in the Control Panel allows you to create Active and Standby partitions, as well as to reconfigure existing file systems. You can also use the Control Panel to delete file systems.



Deleting the file system erases all data stored on the System Director.

For information on creating partitions, see the *Avid ISIS Setup Guide*.

Reconfiguring the File System

You can reconfigure the internal memory configuration of the System Director — for example, if you want to adjust the memory usage to take advantage of expanded memory capabilities. Reconfiguring the file system entails the following:

- Validating the export file
- Creating new metadata
- Importing the metadata



Reconfiguring an existing file system does not delete any data.

To reconfigure the file system:



1. On the Control panel, click Stop System Director.

A dialog box opens, prompting you to confirm that you want to stop the System Director.

2. Click OK.

The System Director Shutdown dialog box opens stating that it is saving multiple copies of the metadata.

3. Click the File System tab, if it is not selected.

4. In the “Active File System Actions” section, click “Reconfigure File System.”

A dialog box opens, prompting you to confirm that you want to reconfigure the existing file system.

5. Click OK.

The system reconfigures its metadata and restarts the System Director.

Creating or Re-creating a File System

You might need to create or re-create a file system if you are:

- Setting up a System Director for the first time
- Adding a second System Director
- Upgrading your System Director hardware
- Deleting and re-creating the System Director file system to recover from an error

For more information about creating, deleting and re-creating file systems on the System Director, see the *Avid ISIS Setup Guide*.

Monitoring Metadata Status

The System Director Status panel displays information about the System Director’s internal description of the file system. This metadata memory is used to record descriptions of Workspaces, folders, and files.



All of this metadata information is also displayed in the ISIS Launch Pad.

To guard against corruption of the metadata due to a system failure, the metadata is saved to disk every 20 seconds. The metadata save operations alternate between two files, Partition0 and Partition1. This guarantees the existence of one known good file if a failure occurs while writing to one of the files. The System director automatically chooses the best copy to load when it starts up.

Metadata memory is also saved automatically to the Partition0 and Partition1 files when the System Director stops normally and without error. A third file, PartitionDump.bin, containing an alternate representation of the file system metadata is also created. The PartitionDump.bin file should be used only when adding memory to a System director or moving to a newer System Director with more memory, unless otherwise instructed by Avid Customer Support.

The Metadata Status box shows when the metadata was last verified and saved, and replicated. A green indicator means no problem has been detected. A yellow indicator means the status is uncertain. A red indicator means that a problem exists.

The following tables lists the status messages displayed in the Metadata Status box.

Status Category	Messages	Additional Notes
Overall Status	- Metadata loaded - Validating - No Metadata loaded - Loading nn.n MBps - State Unknown	System Director is running Occurs periodically System Director is stopped or metadata is unable to load for some reason System Director is restarting
Verification	- Not Active - Verified - Verify Failed - State Unknown	When the System Director is in standby mode, the Verify indicator is disabled.
Saving	- Saving - Saved - Unknown State - Not Active - Save Failed	
Replication	- Sending - Receiving - Unknown State - Not Active - Replication Failed	When the System Director is not in a Dual System Director configuration, the Replicate indicator is disabled.

Creating a Metadata Dump File

You can use the “Dump Metadata” function to write all metadata information to a text file.



This operation should be used only as a diagnostic aid. You cannot restore ISIS metadata from a metadata dump file.



When you write metadata to a file, the resulting file is extremely large and takes a long time to create. Do not use this option unless instructed to do so by Avid Customer Support.

To write the contents of metadata to a text file in the System Director directory:



- In the System Director toolbar, click Dump Metadata.

A text file called PartitionDump.txt is created in the System Director’s data directory:

"D:\Program Files\Avid\ISIS System Director"

Resetting the Administrator Password

The Control Panel allows you to reset the ISIS administrator's password in the event that it is forgotten. This feature does not affect the Windows operating system password. Windows administrator's privileges are required to reset the password.



To change the administrator's password, use the ISIS Management Console. For more information, see "Changing the Administrator Password" on page 29.

To reset the administrator's password:



1. In the Control Panel toolbar, click Reset ISIS Password.

A dialog box warns you that this action removes the administrator's password from the System Director's account.

2. Click Yes to clear the password.

Managing Active Clients

The Active Clients tab displays the identity of the Avid ISIS clients known to the System Director. Use the information listed in this tab to determine if obsolete numeric identifiers (IDs) exist in the System Director.

File System Dual System Director Active Clients						
Name	ID	Type	OS	License	Last Seen	
localhost	0	SystemDirector	Windows	0		
stingraydoc_sm0	1	StorageManager	Windows	0	Mon Feb 24 14:20:23 2014	
stingraydoc3236	2001	Admin	Windows	0	Mon Feb 24 14:20:45 2014	
stingraydoc4680	2002	Admin	Windows	0	Mon Feb 24 14:20:47 2014	
stingraydoc4668	2003	Admin	Windows	0	Mon Feb 24 14:20:47 2014	
stingraydoc1512	2004	Admin	Windows	0	Mon Feb 24 14:20:45 2014	
stingraydoc2124	2005	Admin	Windows	0	Mon Feb 24 14:20:34 2014	

0 of 90 Licenses in use

Refresh Disconnect

The Active Clients tab displays all active Storage Managers as well as connected client accounts. You can use the Bandwidth dialog box in the ISIS Management Console to view only the active client accounts. For more information, see ["Monitoring Client Bandwidth" on page 110](#).

The System Director reports the current client status as described in the following table.

Heading	Description
Name	Name of the client
ID	An internal numeric identifier used by the System Director to represent each client that has a Workspace mounted. These identifiers are assigned when a client first contacts the System Director and remain valid until the client unmounts all Workspaces

Heading	Description (Continued)
Type	Client type (Admin, Client, Storage Manager or System Director)
OS	Operating system on the client
License	Number of licenses registered to the client
Last seen	Date and time when each client last sent its status to the System Director. The System Director removes the entry when all Workspaces are unmounted from the client desktop

The area below the active clients list indicates the number of licenses being used by the clients currently connected to the shared storage network.

If a client fails without unmounting all Workspaces, the System Director maintains the numeric identifiers. Typically, this is not a problem because the same identifier is reused when that client mounts a Workspace the next time. However, it is possible for a client to leave a Workspace mounted, shut down the client system, and never be seen by the System Director again. If that client system is then physically removed or renamed, the numeric identifiers are not removed from the identification table. If enough obsolete entries accumulate, new clients might not be able to obtain numeric identifiers.

To check the license status of an active or an inactive client:

- ▶ Select the client in the active client list, and click Refresh.

To disconnect an active or an inactive client:

- ▶ Select the client in the active client list, and click Disconnect Client.



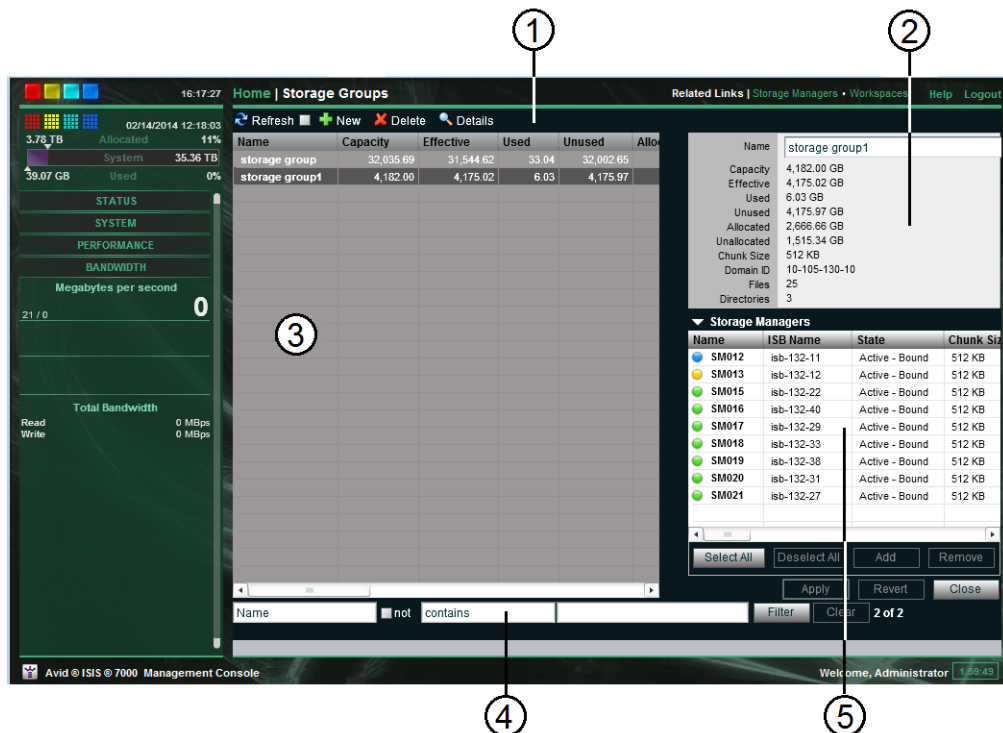
Inform the client you are temporarily disconnecting them and that the connection will return after a few seconds.

5 Managing Storage Groups and Workspaces

Storage Groups are collections of Storage Managers. Storage Groups give you flexibility in allocating storage capacity among groups with different functional areas, workflow requirements, or as a means of mitigating the risk of various drive failure scenarios. Workspaces are virtual volumes that exist on Storage Groups and can be resized dynamically. Workspaces allow you to segment your Storage Groups easily to accommodate projects and users.

Managing Storage Groups

The Storage Groups page of the ISIS Management Console allows you to add and delete Storage Groups, to rename Storage Groups, and to configure and manage Storage Groups.



- 1 Action button toolbar—Perform actions on selected Storage Groups
- 2 Details panel—Detailed information on the selected Storage Groups; see [“Viewing Storage Group and Storage Manager Details” on page 62](#)
- 3 Storage Groups list—Lists all configured Storage Groups and related information; see [“Storage Groups List” on page 62](#)
- 4 Filter panel—Filter the Storage Groups list display based on conditions you configure; see [“Filtering the Display” on page 24](#)
- 5 Storage Managers list—Displays Storage Managers bound to the selected Storage Group

Storage Groups List

The following table summarizes the information available in the Storage Groups list. This information is also displayed in the Details panel for a selected Storage Group.

Heading	Description
Name	Displays the name of the currently selected Storage Group
Capacity	Displays the storage capacity in gigabytes (GB) of the selected Storage Group
Effective	Displays the effective (available) storage capacity in gigabytes (GB) of the selected Storage Group
Used	Displays the amount of storage space in gigabytes (GB) that currently has data written on it in the selected Storage Group
Unused	Displays the total amount of storage space in gigabytes (GB) that currently has no data written on it in the Storage Managers assigned to the selected Storage Group
Allocated	Displays the amount of storage space in gigabytes (GB) reserved for use by Workspaces in the selected Storage Group
Unallocated	Displays the amount of storage space in gigabytes (GB) available on the Storage Managers and not currently reserved for the selected Storage Group
Chunk Size	Displays the size of segmented media files sent over the network
Files	Displays the number of files in the selected Storage Group
Directories	Displays the number of directories in the selected Storage Group

You can sort the information in the Storage Groups page by clicking any column heading. For more information on sorting items in columns, see [“Sorting Information” on page 24](#).

Viewing Storage Group and Storage Manager Details

The Details and Storage Managers panels display information about the currently selected Storage Group and the Storage Managers it contains. The information displayed is the information as seen by the System Director. Some of the information is embedded in the Storage Manager, and other information is assigned to the Storage Manager by the Avid ISIS software.



To sort the information in the Storage Managers panel, click any column heading. For more information on sorting items in columns, see [“Sorting Information” on page 24](#).

To view information about a Storage Group:

- In the Storage Groups list, select a Storage Group.

The Storage Groups page displays all the information for the selected Storage Group. If the Details panel is not visible, click Details.

To close the Details panel:

- Click Details.

The Storage Managers panel lists the Storage Managers allocated to the currently selected Storage Group, as well as the Storage Managers available for allocation to the Storage Group.

For information about what is shown in the Storage Managers panel, see [“Storage Manager Column List” on page 34](#). Some columns are hidden by default (see [“Showing and Hiding Columns” on page 24](#)).

Storage Groups on ISIS | 7500

Storage Groups are created from bound Storage Managers. First, you bind Storage Managers to the system, then you create one or more Storage Groups using the Storage Managers. A Storage Manager can belong to only one Storage Group. After you create a Storage Group you can create Workspaces.

Storage Groups and Chunk Sizes

Storage Managers are combined to create Storage Groups in the ISIS file system. When you bind a Storage Manager you must select either 512 KB (default) or 256 KB chunk sizes. Earlier Avid ISIS releases used 256 KB chunk sizes. These bound Storage Managers must all be of the same chunk size when you configure your Storage Group.



Avid ISIS switch hardware shipped with v1.x (ISS1000 and IXS1000) does not support 512 KB chunk sizes. If you have Avid ISIS v2.x software running on v1.x switches, you must select the 256 KB chunk size when adding Storage Managers to the file system to create Storage Groups.

You cannot change the chunk size of an existing Storage Group. If you need to change the chunk size of a Storage Group, you must delete it and create a new one with the desired chunk size, using Storage Managers that use that chunk size. The chunk size selection is available only when binding the Storage Managers.

Storage Managers and Chunk Sizes

All Avid ISIS | 7500 ISBs contain two drives, and are identified by the total amount of storage in the ISB; for example, an ISB with two 1 terabyte (TB) drives is called an i2000. The supported chunk size available on each ISB type is listed below:

- 256 KB—i500 and i1000 only
- 512 KB—All (i500, i1000, i2000, i4000, i8000); Requires v2.x switch hardware (ISS2000 and IXS2000)

RAID-6 Workspace, Single ISB Failure

When there is a single ISB failure in an ISIS Workspace configured with RAID-6 protection, the Workspace continues to function normally but at a lower bandwidth. For more information, see [“Mirrored Workspace, Single ISB Failure” on page 64](#).

After confirming the failure of an ISB, Avid highly recommends that you initiate the remove redistribution process immediately. There are two benefits to doing this:

- Immediately upon initiation of the remove redistribution, all new writes to the Workspace have the full benefit of RAID-6 protection (dual-parity protection).
- Upon completion of the remove redistribution process, existing data in the Workspace is once again fully protected. Prior to completion, if another ISB were to fail, the Workspace would be in an unprotected state (though no data would be lost).

RAID-6 Workspace, Dual ISB Failure

An “unprotected state” occurs if two ISBs fail in a RAID-6 Workspace. In an unprotected state with no additional failures, read operations continue to function normally at a lower bandwidth.

However, in an unprotected state, due to the distributed architecture of the ISIS file system (optimized for real-time performance), it is possible under certain circumstances that the system would not be able to correctly update the parity information when writing new data. As a result under these circumstances, the file system could return a failure status when writing. While the failure rate percentage on the total number of write operations is low, heavy workloads on the system would result in enough write failures to disrupt operations.

This issue only applies when the Workspace is in an unprotected state and the remove redistribution process on the failed ISBs has not been initiated. Therefore, Avid highly recommends that you initiate the remove redistribution process immediately upon confirmation of any ISB failure. This ensures immediate protection (RAID-6 or mirroring) of new data being written, and full protection of all stored data at the earliest possible time.

Mirrored Workspace, Single ISB Failure

An “unprotected state” occurs when you have a single ISB failure in a mirrored Workspace. In an unprotected state with no additional failures, read operations continue to function normally.

However, in an unprotected state a subsequent or infrastructure failure will cause operational issues which could result in failures when writing new data or prevent you from accessing data in the Workspace. An additional ISB failure can compromise data accessibility. Networking issues, on the other hand, will not cause accessibility issues on previously written data but might prevent the successful completion of an active write operation.

This issue only applies when the Workspace is in an unprotected state and the remove redistribution process on the failed ISBs has not been initiated. Therefore, Therefore, Avid highly recommends that you initiate the remove redistribution process immediately upon confirmation of any ISB failure. This ensures immediate protection (RAID-6 or mirroring) of new data being written, and full protection of all stored data at the earliest possible time.

Matching Chunk Sizes to the File System

If you add an ISB (displays as an available Storage Manager) to your file system, make sure you match the chunk size of the new Storage Manager to the chunk size of the existing Storage Group. New Storage Managers are added with a default chunk size of 512 KB on mirrored Storage Groups (256 KB with i1000 ISBs). You cannot mix the chunk sizes within a Storage Group. To change the chunk size of an ISB, you must remove the Storage Manager from the file system and add the Storage Manager again (rebind it), selecting the same protection and chunk size as the existing Storage Group.

Zone 1 Switches

The ISIS v2.x generation IXS and ISS switches install in the same engines as earlier releases; the chassis has not changed. However, all the switches in the engines must be of the same generation. The two new switches are labeled IXS2000 and ISS2000. The new switches cannot be mixed in ISIS Engines with earlier versions of the switches (labeled IXS1000 and ISS1000). If your IXS and ISS switches are not labeled, consider them the earlier versions. The ISS2000 switches are required for 10 Gb clients and 512 KB chunk size, see [“Storage Groups and Chunk Sizes” on page 63](#).

The Avid ISIS documentation refers to IXS2000 and ISS2000 switches as v2.x hardware and IXS1000 and ISS1000 switches as v1.x hardware.

Storage Groups on ISIS | 5500 and ISIS | 2500

For both ISIS | 5500 and ISIS | 2500, each Engine is a Storage Manager. You can assign all of your Engines to one large Storage Group, or each Engine can be a Storage Group. An Engine can be assigned to only one Storage Group.

Avid ISIS | 5500 provides RAID-5 data protection with an active hot spare and Avid ISIS | 2500 provides RAID-6 data protection.

Adding Storage Managers to Storage Groups

You can add unassigned Storage Managers to a Storage Group to increase its storage capacity. This is typically done when adding a new Engine to your Avid ISIS system. This process initiates a redistribution of the files in the existing Storage Group to include the new Storage Manager. For more information, see [“Redistributing Data” on page 81](#).

To add Storage Managers to a Storage Group:

1. From the Management Console home page, click Storage Groups in the System section.

The Storage Groups page opens.

2. In the Storage Groups list, select the Storage Group where you want to add Storage Managers, and then do one of the following:

- ▶ Click Details.
- ▶ Double-click the Storage Group name.

The Details panel displays all the information on the selected Storage Group.

3. In the Storage Managers panel, select all the spare Storage Managers you want to add to the Storage Group.



If you have two Management Domains in the ISIS | 7500, check the Domain ID column and select Storage Managers from the same domain. You cannot add Storage Managers to a Storage Group with a different Domain ID. Storage Groups cannot span Management Domains.

4. Click Add to add the selected spare Storage Managers to the Storage Group.

The Storage Managers panel refreshes to display the selected Storage Managers added to the Storage Group.

5. (Option) Click Revert to undo any modifications made to the Storage Group information.
6. Click Apply.

The Storage Managers are added to the Storage Group.

- The shared storage network performs a redistribution of any data on the Storage Managers. The amount of time required for the redistribution depends on the amount of data in the Storage Group.
- The configuration change counter for all affected Workspaces is incremented by one.



After 20 configuration changes, the system advises you to perform a full redistribution. You can suspend and resume the redistribution as needed. For more information, see [“Suspending and Resuming Redistribution” on page 85](#).

Creating New Storage Groups

A Storage Group is a set of physical Storage Managers that store a subset of the complete set of media files accessible within a shared storage environment. You can create up to 32 Storage Groups.



You must add Storage Managers to the file system before you can create any Storage Groups. For more information, see [“Binding Storage Managers to the ISIS File System” on page 38](#).



If you have bound Storage Managers to the ISIS file system but you have not created any Storage Groups, the Create Storage Groups dialog box opens by default when you select the Storage Groups list.

To create a new Storage Group:

1. From the Management Console home page, click Storage Groups in the System section.
The Storage Groups page opens.
2. Click New.
The Create Storage Group dialog box opens.
3. In the Name text box, type a name for the Storage Group.



For information on valid and invalid characters, see “Entering Text” on page 26.

4. In the Storage Managers panel, select the Storage Managers you want to assign to the new Storage Group.
5. Click Add.
The Storage Managers are allocated to the Storage Group. You can click Remove to remove Storage Managers from the Storage Group.
6. (Option) Before you create your Storage Group, you can click Revert to undo any modifications made to the Storage Group information.
7. Click Apply to create a new Storage Group containing all the selected Storage Managers.
If there is already a Storage Group with the same name, an error message is displayed.
The new Storage Group appears in the Storage Groups list, and the Create Storage Group dialog box refreshes to show the Storage Managers still available for additional Storage Groups.
8. (Option) Repeat steps 3 through 8 to create new Storage Groups.
9. Click Close to close the Create Storage Group dialog box and to return to the Storage Groups page.

Removing ISIS Storage Managers from Storage Groups

You can remove Storage Managers from your Storage Group, as long as the following conditions continue to apply after the operation:

- The Storage Group contains at least the minimum number of Storage Managers remain. For more information, see “Creating New Storage Groups” on page 65.
- If the ISIS | 7500 Storage Group includes RAID-6 Workspaces in the Storage Group, you must have at least 8 Storage Managers in the Storage Group.
- The Storage Group contains enough Storage Managers to support the space allocated to your Workspaces.



This is the total amount of storage allocated to the Workspaces, not the actual amount of data stored on the Workspaces.

Storage Managers removed from the Storage Group are returned to the system’s pool of spare Storage Managers.



When Storage Managers are removed, a redistribution is initiated. If you start the Storage Manager removal during high client usage, it might reduce performance on your clients. This can include dropped frames, underruns, and failed captures. Remove Storage Managers during periods of light client activity.

You can suspend and resume a redistribution as needed.

To remove Storage Managers from a Storage Group:

1. From the Management Console home page, click Storage Groups in the System section.
The Storage Groups page opens.

2. In the Storage Groups list, select the Storage Group from which you want to remove Storage Managers, and then do one of the following:
 - ▶ Click Details.
 - ▶ Double-click the Storage Group name.

The Details panel displays all the information on the selected Storage Group.

3. In the Storage Managers panel, select all the Storage Managers you want to remove from the Storage Group.
4. Click Remove.

The Storage Managers panel refreshes and displays the selected Storage Managers as Spare.



You cannot remove Storage Managers if it would cause the capacity of the Storage Group to fall below either the used space or the allocated space. You must reduce the amount of space allocated to the Workspaces. For more information on modifying Workspaces, see “Resizing Workspaces” on page 78.

5. (Option) Click Revert to undo any modifications made to the Storage Group information.
6. Click Apply.

The Storage Managers are added to the Storage Group.

Adding Storage Managers from Another Storage Group

If you want to reassign Storage Managers from one Storage Group to another, you must remove the Storage Managers from the current Storage Group before adding them to a new one.

To add Storage Managers previously used in another Storage Group to your current Storage Group:

1. From the Management Console home page, click Storage Groups in the System section.
The Storage Groups page opens.
2. In the Storage Groups list, select the Storage Group which contains the Storage Managers you want to reassign, and then do one of the following:
 - ▶ Click Details.
 - ▶ Double-click the Storage Group name.
 The Details panel displays all the information on the selected Storage Group.
3. In the Storage Managers panel, select all the Storage Managers you want to move to another Storage Group.
4. Click Remove.
The Storage Managers panel refreshes to display the selected Storage Managers as Spare.
5. Click Apply.
The selected Storage Managers are removed from the Storage Group, and the shared storage network performs a redistribution of any data on the Storage Managers.
6. In the Storage Groups list, click the Storage Group to which you want to add the Storage Managers.
The Details panel displays all the information on the selected Storage Group.
7. In the Storage Managers panel, select all the spare Storage Managers you want to add to the new Storage Group.



If you have two Management Domains, check the Domain ID column and select Storage Managers from the same domain. You cannot add Storage Managers to a Storage Group with a different Domain ID. Storage Groups cannot span Management Domains.

8. Click Add to add the selected Storage Managers to the Storage Group.

The Storage Managers panel refreshes to display the selected Storage Managers added to the new Storage Group.

9. (Option) Click Revert to undo any modifications made to the Storage Group information.

10. Click Apply.

The selected Storage Managers are added to the Storage Group, and the shared storage network performs a redistribution of any data on the Storage Managers. The amount of time required for the redistribution depends on the amount of data in the Storage Group.

Adding Storage Managers From Another Environment (ISIS | 7500)

If adding Storage Managers that were previously used in another environment, first connect them to your Avid ISIS shared storage network, and then bind them to the ISIS using the Storage Manager page.

To add the Storage Managers to your current Storage Group:

1. Make sure the new Storage Managers are connected to the network. For information on connecting Storage Managers, see the *Avid ISIS Setup Guide*.
2. Open the ISIS Management Console. (For information on opening the ISIS Management Console, see [“Opening the Management Console” on page 15.](#))
3. Click Storage Manager in the System panel.

The Storage Manager page opens.

If the ISIS Management Console was open when you added the Storage Manager, click Refresh to view the newly added Storage Manager.

If the Storage Managers are not listed, something might be wrong with their physical connections; see the *Avid ISIS Setup Guide*.

4. Add the new Storage Managers to your Storage Group (see [“Adding Storage Managers to Storage Groups” on page 65](#)).
5. Click Apply.
6. Click Yes.

A dialog box opens asking you to confirm the action.

The selected Storage Managers are added to the Storage Group.

Deleting Storage Groups

You can delete any Storage Group that does not have any Workspaces on it. As a result, all Storage Managers previously assigned to the Storage Group return to the system’s pool of spare Storage Managers.

To delete a Storage Group:

1. If any Workspaces exist on the Storage Group you want to delete, first delete the Workspaces (see [“Deleting Workspaces” on page 79](#)).
2. From the Management Console home page, click Storage Groups in the System section.
3. In the Storage Groups list, select the Storage Group you want to delete.
4. Click Delete.

A dialog box opens asking you to confirm the action.

5. Click Yes.

The Storage Group is deleted.

After the Storage Group is deleted, all of the Storage Managers previously in your Storage Group will appear in the Storage Managers panel as Spare.

Minimum Free Storage Space Requirement

Avid recommends that you maintain a minimum threshold of free space in each Storage Group. The amount differs depending on the ISIS model:

- On the ISIS | 7500, keep at least 7% of free space in each Storage Group. Exceeding 93% used space can produce severe performance issues in some situations.
- On the ISIS | 5500 and ISIS | 2500, keep at least 5% of free space in each Storage Group.

To calculate the right amount of free space, log into the ISIS management Console and navigate to the Storage Group window. For each Storage Group, multiply the Effective number by 0.07 or 0.05 (depending on your ISIS system) to determine your recommended free space in GBs. Create a new workspace of that size in this Storage Group and label it “Headroom” and do not give anyone access to this workspace.

Managing Workspaces

This section describes how to create, rename, and delete Workspaces. and how to manipulate the amount of storage allocated to each Workspace.

The screenshot shows the ISIS management console interface. The main window is titled 'Storage Group' and contains a table of workspaces on the left and a details panel on the right. The table has columns for Name, Capacity, and a progress bar. The details panel shows information for 'workspace1', including its capacity, used space, and user access settings. Numbered callouts 1 through 5 point to specific UI elements:

- 1: The 'Refresh' button in the top toolbar.
- 2: The 'Name' field in the details panel.
- 3: The 'Capacity' column header in the workspace table.
- 4: The 'Filter' button at the bottom of the workspace table.
- 5: The 'Apply' button in the 'User Access' section of the details panel.

The workspace table lists various workspaces, including workspace8, workspace7, workspace6, workspace5, workspace4, workspace3, workspace2, workspace1, workspace, 23, _Shared Project, WS5, WS4, WS3, WS2, WS1, Stan_cant_spell, Gus, Stan, Capture workspace, workspace14, workspace13, workspace12, and workspace11. The details panel for 'workspace1' shows a capacity of 200.00 GB, with 0.00 GB used and 200.00 GB unused. The 'User Access' section shows a table of users and their access levels.

Name	Type	Access	Effective
user1	User	Read	Read
user3	User	Read	Read
Guest	User	None	None

1	Action button toolbar—Perform actions on selected Workspaces
2	Details panel—Detailed information on the selected Workspaces; see “Viewing Workspace Details” on page 73
3	Workspaces list—Lists all configured Workspaces and related information; see “Workspaces List” on page 70
4	Filter panel—Filter the Workspaces list display based on conditions you configure; see “Filtering the Display” on page 24
5	User access panel—Displays users who have access to the selected Workspace and details about their access privileges; see “Managing Workspace Access Privileges” on page 80

Workspaces List

The Workspaces list displays all Workspaces, the Storage Groups on which they reside, and details about each Workspace.

Heading	Description
Name	Lists the names of all Workspaces in the selected Storage Groups
Capacity	Lists the total storage capacity of each Workspace in gigabytes (GB)
Resize slider	Displays a graphical representation of the used and available space for each Workspace (for information on using the Workspace Size graph, see “Using the Workspace Size Graph” on page 72)
Maximum	Lists the maximum amount of storage space in gigabytes (GB) available for the Workspace on the network
Protection Mode	Displays the type of protection applied: Avid ISIS 7500 provides “mirrored” and “RAID-6” data protection modes, as well as an “unprotected” mode. Avid ISIS 5500 provides RAID-5 data protection with an active hot spare, called “HW RAID.” Avid ISIS 2500 provides RAID-6 data protection, called “SW RAID.”
Used	Displays the amount of storage space in gigabytes (GB) that currently has data written on it in each Workspace
% Used	Displays the percentage (%) of storage space currently storing data on the Workspace
Reserved	Displays the amount of storage space in gigabytes (GB) that has been reserved by a client application
Unused	Lists the amount of storage space in gigabytes (GB) that currently has no data written on it in each Workspace
Status	Displays the status of any current redistribution: • In Progress • Stalled • Pending • Suspended • Requires Full Redistribution
Config Changes	Displays the number of changes to a Storage Group that involve moving data — for example, the number of times a Storage Manager has been added or removed
Storage Group	For each Workspace, lists the Storage Group on which it is located

Heading	Description
Files	Lists the total number of files stored on the network for each Workspace



To sort the information in the Storage Managers panel, click any column heading. For more information on sorting items in columns, see “Sorting Information” on page 24.

Workspace Considerations

Before you create Workspaces:

- Consider how you want to allocate them. For example, do you want to allocate them to accommodate projects, groups, individual clients, streaming bit rates, media types, media distributors, or a combination of these?
- Determine how much storage each Workspace requires and allocate space accordingly. This might be a function of project size or the number of clients, or it might be a function of media duration or media resolution.
- On ISIS | 7500 systems, consider the chunk size implications. Workspaces can be moved only to Storage Groups with the same or a larger chunk size.

In a multiple Workspace configuration, consider reserving some space rather than assigning all of it immediately. Once space is allocated, it tends to be filled quickly and you might need space later to accommodate a new project or client or to extend or protect an existing Workspace. In these situations, it is easier to use space held in reserve than to take it away from an existing Workspace.

When allocating and sizing Workspaces, also consider whether access restrictions are required and whether protection for data integrity is necessary for each Workspace.

The sections below describe Workspace considerations that apply only to ISIS | 7500 because of the different Workspace protection modes available. On ISIS | 5500, the only data protection mode is hardware RAID; on ISIS | 2500, the only protection mode is software RAID.

Workspace Data Protection (ISIS | 7500 only)

Avid ISIS | 7500 supports two types of Workspace data protection: mirrored and redundant array of independent disks (RAID-6), which in turn depends on the number of Storage Managers in the Storage Group:

- For Mirrored Workspaces there must be at least two Storage Managers in the Storage Group
- For RAID-6 Workspaces there must be at least eight Storage Managers in the Storage Group, and the Chunk Size must be 512 KB. RAID-6 storage provides more storage at a lower cost per GB.

Workspace Creation (ISIS | 7500)

The following table describes what protection modes you can apply to a Workspace in a Storage Group on an ISIS | 7500 depending on what the Storage Group already contains.

If the Storage Group contains:	You can create:
No Workspaces	Mirrored, unprotected, or RAID-6 Workspaces
Unprotected Workspaces	Mirrored or unprotected Workspaces
Mirrored Workspaces	Mirrored or unprotected Workspaces
RAID-6 Workspaces	RAID-6 Workspaces (only)

Workspace Duplication (ISIS | 7500)

You can duplicate a Workspace in a Storage Group on an ISIS | 7500 that supports the same protection mode as the source Workspace, as described in the following table.

Protection Mode of Workspace to Duplicate:	Target Storage Group can Contain:
Unprotected Workspace	Mirrored, unprotected, or no Workspaces
Mirrored Workspaces	Mirrored, unprotected, or no Workspaces
RAID-6 Workspaces	RAID-6 or no Workspaces

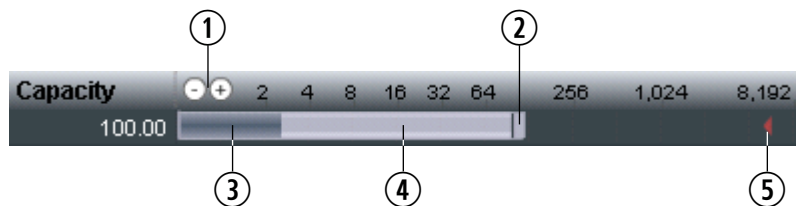
Workspace Moves (ISIS | 7500)

You can move a Workspace to a Storage Group with the same protection mode as the Workspace you are moving. For any selected Workspace, the Storage Groups list displays only other Storage Groups with the appropriate protection mode: if you select a RAID-6 Workspace, only Storage Groups that support RAID-6 workspaces appear in the list. If the Workspace is mirrored, only Storage Groups that support mirrored or unprotected Workspaces appear in the list.

Using the Workspace Size Graph

The Workspaces Size graph provides a quick way to view how much storage capacity is currently allocated to each Workspace and how much of that storage space currently has data written on it. The graph represents the following:

- Workspace size—total drive space in the Storage Group allocated to each Workspace
- Used space—used drive space in the Workspace
- Unused space—unused drive space in the Workspace
- Maximum Workspace size—total of Workspace size + drive space in the Storage Group still available for allocation to each Workspace



- | | |
|---|--|
| 1 | Decrease/Increase buttons—Increases or decreases the scale of the graph |
| 2 | Resize handle—Click and drag to increase or decrease the Workspace size; see “Resizing Workspaces” on page 78 |
| 3 | Used Space |
| 4 | Unused space |
| 5 | Maximum Workspace size—total of Workspace size + drive space in the Storage Group still available for allocation to each Workspace |

To resize the Workspaces Size graph, do one of the following:

- Click Decrease Size to reduce the size of the graph.
- Click Increase Size to expand the size of the graph.

Viewing Workspace Details

The Details panel and the User Access panels display all information for the currently selected Workspace.

To view detailed information about a Workspace:

- In the Workspaces list, select a Workspace.

The Workspaces page displays all the information for the selected Workspace. If the Details panel is not visible, click Details.

To close the Details panel:

- Click Details.

The Details panel contains the same information as the Workspaces column list (except for the Resize slider and the Maximum storage space; see [“Workspaces List” on page 70](#)), but includes the following additional information:

Heading	Description
Directories	Displays the number of directories used by the selected Workspace
Warning Event Trigger	Displays the value in used percentage (%) or unused gigabytes (GB) of storage at which a warning event is written to the Event Log
Error Event Trigger	Displays the value in used percentage (%) or unused gigabytes (GB) of storage at which an error event is written to the Event Log
Chunk Size	The smallest unit of data that can be written to the disks

The User Access panel lists all users and user groups and their access privileges. (For information on access privileges, see [“Managing Workspace Access Privileges” on page 80](#).)

Heading	Description
Name	Lists the names of the users and user groups on the network
Type	Displays the client category (user or user group) for each client in the Name list
Access	Lists the access privileges for each client in the Name list
Effective	Lists the effective access privileges for each client in the Name list
Reason	Lists the reason for any difference between the access privileges assigned to a user and the effective access assigned to a user as a member of a user group



To sort the information in the User Access panel, click any column heading. For more information on sorting items in columns, see [“Sorting Information” on page 24](#).

Adding New Workspaces

Workspaces are locations to store and segregate data. You can allow users to access some or all of the Workspaces, and you can assign permissions for how each user can access the data in a Workspace. You can create up to 1024 Workspaces, divided among all your Storage Groups.



If you have created Storage Groups but you have not created any Workspaces, the Create Workspace dialog box opens by default when you select the Workspaces list.

To add a new Workspace:

1. From the Management Console home page, click Workspaces in the System section.

The Workspaces page opens.

2. Click New.

The Details panel opens.

3. In the Name text box, type a name for the Workspace.



For information on valid and invalid characters, see “Entering Text” on page 26.

4. Click the Storage Group menu, and select the Storage Group in which you want to create the Workspace.

The Storage Group name appears in the Storage Group text box.

5. (ISIS | 7500 Option) Click the Protection menu and select a Workspace protection option (depends on the protection modes available for the Storage Group you selected).

6. Type a size for the Workspace in the Capacity text box. The default size (200 GB) is listed in the Capacity text box, and the maximum size is listed next to the Capacity text box.



The minimum Workspace size is 1 GB.

If all storage in the Storage Group is allocated to existing Workspaces, you can make an existing Workspace smaller. For information on resizing Workspaces, see “Resizing Workspaces” on page 78.

7. (Option) To set a Warning event trigger, select the type of trigger from the drop-down list (either Used % > or Unused GB <), then type in a value.
8. (Option) To set an Error event trigger, select the type of trigger from the drop-down list (either Used % > or Unused GB <), then type in a value.



For more information about setting Event triggers, see “Setting Event Triggers” on page 78.

9. In the User Access panel, set the User and User Group access privileges (for more information, see “Setting Workspace Access Privileges” on page 81).

10. Click Apply.

The new Workspace appears in the Workspace dialog box, and the Create Workspace dialog box refreshes to allow you to create a new Workspace.

If there is already a Workspace with the same name, an error occurs.

11. (Option) Repeat steps 3 through 10 to create new Workspaces.
12. Click Close.

The new Workspace appears in the Workspaces list.

Duplicating Workspaces

When you duplicate Workspaces, they inherit the attributes of the Workspace from which they were created.



The contents of the original Workspace are not duplicated.

To duplicate a Workspace:

1. From the Management Console home page, click Workspaces in the System section.

The Workspaces page opens.

2. In the Workspace list, select the Workspace you want to duplicate.
3. Click Duplicate.

The Duplicate Workspace dialog box opens.

4. (Option) Modify any of the attributes of the new Workspace. For information on modifying Workspaces, see the following topics:

- [“Resizing Workspaces” on page 78](#)
- [“Renaming Workspaces” on page 75](#)
- [“Protecting ISIS | 7500 Workspaces” on page 76](#)
- [“Managing Workspace Access Privileges” on page 80](#)

5. Click Apply.

The duplicate Workspace appears in the Workspace list, and the Duplicate Workspace list refreshes to allow you to duplicate a new Workspace. The new Workspace has a default name — Workspace n , where n is an integer that is incremented each time you click Apply to create another duplicate Workspace.

If there is no room for a Workspace of the same size as the original, the Capacity column displays a red line and the Apply button remains inactive.

6. Click Close.

Renaming Workspaces

You can rename a Workspace at any time, even when it is being used by client workstations and mapped to a local drive or by letterless mapping (to a Universal Naming Convention path) on the client system. The only effect on users is that the Workspace name will be different the next time they need to access it.

To rename a Workspace:

1. From the Management Console home page, click Workspaces in the System section.

The Workspaces page opens.

2. In the Workspaces list, click the Workspace name you want to change.
3. If the Details panel is not visible, do one of the following:

- ▶ Click Details.
- ▶ Double-click the Workspace name.

The Workspaces Details panel displays all the information on the selected Workspace.

4. Type a new name in the Name text box.



For information on valid and invalid characters, see [“Entering Text” on page 26](#).

5. (Option) Click Revert to undo any modifications made to the Workspace information.
6. Click Apply.

Protecting ISIS | 7500 Workspaces

Because of the potential impact of a drive failure, Avid recommends protecting all your Workspaces whenever possible. On the ISIS | 7500, workspace protection is optional. If you want to ensure protection of your files at all times, always choose a Protection option when creating new Workspaces (before any files are stored on the Workspace).

If you are not sure that all files on a given Workspace are protected, select the Workspace and enable the available Protection option for the Workspace. This protects all new files added to the Workspace, and adds protection to any existing files in the Workspace that are not already protected. Using RAID-6 protection on Workspaces has the following advantages:

- Migration from mirrored to RAID-6 Workspaces can become part of your normal workflow. You can move the data that is no longer used in the mirrored Workspaces to RAID-6 Workspaces for long term storage. This frees up faster Storage Managers for higher performance work.
- RAID-6 Workspaces allow you to use low bit-rate data, at less cost.

The following table summarizes the advantages and disadvantages of the different protection types:

Type	Advantages	Disadvantages
Mirrored	• Maximizes performance of protected Workspaces • Supports high-resolution workflows	• Mirrored Workspaces use twice as much space as unprotected Workspaces • Tolerates single Storage Manager failure
RAID-6	• Maximizes protected storage capacity • Tolerates two Storage Manager failures	• Supports low bit-rate (≤ 50 Mbs) workflows

RAID-6 Workspaces have the following restrictions:

- Require a Storage Group with a 512 KB chunk size (256 KB chunk sizes are not supported).
- Require a Storage Group with at least 8 Storage Managers.
- Require ISIS v2.x generation switches (ISS2000/IXS2000) in the ISIS Engines (these switches are also required for 512 KB chunk sizes).
- Support only resolutions that draw 16 MB/s (50 Mb/s) or less.



For example, you can run two streams of DV 50 or DNxHD 36. Bandwidths are listed by resolution and number of streams on the Avid Knowledge Base. Search the Avid Knowledge Base for the Avid ISIS Performance Guide.

- If a RAID-6 Workspace experiences two disk failures, capturing (or writing) to the Workspace is not supported until the error condition is corrected.
- Before you perform a full redistribution, all clients must stop using that Storage Group and unmount the Workspaces in that Storage Group.

Setting ISIS | 7500 Workspace Protection

You can use the Workspaces page to enable or disable Workspace protection.

To enable protection for a Workspace:

1. From the Management Console home page, click Workspaces in the System section.

The Workspaces page opens.

2. In the Workspaces list, click the Workspace you want to protect.

3. If the Details panel is not visible, do one of the following:

- ▶ Click Details.
- ▶ Double-click the Workspace name.

The Workspaces Details panel displays all the information on the selected Workspace.

4. Click Protection menu and select Mirrored.



In order to enable Workspace protection, there must be enough unallocated space in the Storage Group to which the Workspace is assigned. Mirrored protection requires an amount of unallocated space equal to the size of the Workspace.

5. (Option) Click Revert to undo any modifications made to the Workspace information.

6. Click Apply.

Protection is enabled for the Workspace, and the Protection heading changes from unprotected to the type of protection you selected.

To disable protection for a Workspace:

1. In the Workspaces list, click the Workspace from which you want to remove protection.

2. In the Details panel, click the Protection menu and select unprotected from the list to remove protection from the Workspace.

Protection is disabled for the Workspace, and the Protection field for the Workspace changes to Unprotected.

3. Click Apply.

Moving Workspaces

You can move a Workspace and all of its contents by assigning it to another Storage Group in the Details panel of the Workspaces page, as long as the destination Storage Group contains Workspaces using compatible protection modes. For example, you can move a mirrored or unprotected Workspace to a Storage Group that contains other mirrored or unprotected Workspaces, and you can move a RAID-6 Workspace to a Storage Group that contains RAID-6 Workspaces.

On the ISIS | 7500 system, moving a Workspace requires that the destination Storage Group contain Storage Managers of the same or larger chunk size as the source Storage Group.

To move a Workspace to a Storage Group with a smaller chunk size, you must create a new, empty Workspace in the destination Storage Group and manually transfer the files from the source to the destination using an external copy method.



If you are moving between chunk sizes, you cannot do any I/O to the Workspace while the move is in progress. The Management Console displays a warning when you start the move and if you ignore the warning, the I/O fails. You can do I/Os in other Workspaces in both the source and destination Storage Groups during the move.

To move a Workspace and all of its contents to another Storage Group:

1. In the Workspaces list, select the Workspace you want to move.
2. If the Details panel is not visible, do one of the following:
 - ▶ Click Details.
 - ▶ Double-click the Workspace name.

The Workspaces Details panel displays all the information on the selected Workspace.

3. Click the Storage Group menu, and select the Storage Group to which you want to move the Workspace.
4. (Option) Click Revert to undo any modifications made to the Workspace information.
5. Click Apply.

The Workspace is moved, and the Details panel updates to show the new Storage Group assignment. Existing files are moved, and new files written to the Workspace are written to the destination Storage Group.

Resizing Workspaces

There are occasions when you must change the size of Workspaces. For example, you might need to make a Workspace larger to create room for a capture procedure planned for later in the day or for some new media files. Alternatively, you might need to make a Workspace smaller to create space for other Workspaces or to reserve storage for another day.

To adjust the size of a Workspace:

1. From the Management Console home page, click Workspaces in the System section.
The Workspaces page opens.
2. In the Workspaces list, select a Workspace.
3. Do one of the following:
 - ▶ Click the handle of the Workspaces Size graph, and drag it to resize the graphical display. The Workspace size listed in the Capacity text box updates as you drag the handle.
 - ▶ Click Details and type a new value for the Workspace size in the Capacity text box in the Workspace Details panel.
4. Click Apply.



You cannot increase Workspace size above the storage space listed as the maximum size.

Setting Event Triggers

You can set event triggers that will write events to the Event log when Workspace capacity (in gigabytes) is less than the specified value, or when used Workspace capacity exceeds the specified percentage. You can create triggers for both Warning and Error events.

If you have email notifications enabled, you can select the ISIS General Error and Warning subcodes to receive email notifications when Workspace capacity events are written to the Windows Event Log. For more information on email notifications, see [“Configuring the Notification Service” on page 31](#).

To set an event trigger:

1. In the Workspaces list, select the Workspace for which you want to set a trigger.
2. If the Details panel is not visible, do one of the following:

- ▶ Click Details.
- ▶ Double-click the Workspace name.

The Workspaces Details panel displays all the information on the selected Workspace.

3. (Option) Select one of the following from the Warning Event Trigger “used” list:

Option	Description
Unused GB <	Trigger a warning when unused capacity falls below the specified value, in gigabytes
Used % >	Trigger a warning when used capacity exceeds the specified percentage value

4. Type a value in the text field for the used or unused capacity at which you want a warning event to be written to the Event Log.
5. (Option) Select one of the following from the Error Event Trigger “used” list:

Option	Description
Unused GB <	Trigger an error when unused capacity falls below the specified value, in gigabytes
Used % >	Trigger an error when used capacity exceeds the specified percentage value

6. Type a value in the text field for the used or unused capacity at which you want an error event to be written to the Event Log.
7. Click Apply.
8. Click Close.

Deleting Workspaces

You can delete Workspaces that are not currently accessed by any clients. You can also delete Workspaces whether or not they have media files stored on them. You can delete multiple Workspaces at one time.

Before deleting a Workspace, make sure that its media is no longer needed, is moved, or is backed up. You then can safely delete the Workspace.

If you delete a Workspace that has been mapped to a local drive by a client, the client cannot access that Workspace. Clients should unmap the deleted Workspace using the Avid ISIS Client Manager. For information on using the Client Manager, see the *Avid ISIS Client Guide* or the Client Manager Help.



When a Workspace is deleted, a redistribution is initiated. If you start the delete on an ISIS during high client usage, it might reduce performance on your clients. This can include dropped frames, underruns, and failed captures. Delete Workspaces during periods of light client activity.

You can suspend and resume a redistribution as needed.

To delete a Workspace:

1. From the Management Console home page, click Workspaces in the System section.
The Workspaces page opens.
2. In the Workspaces list, select the Workspace you want to delete.
3. Click Delete.

A dialog box opens, prompting you to confirm the operation.

4. Click Yes.

The Workspace is deleted.

Managing Workspace Access Privileges

You can set privileges for user and user group access to Workspaces in the Workspaces page. There are three levels of access available to clients of the network, described in the following table.

Access Level	Description
Read/Write	Workspace can be read and written to.
Read	Workspace can be read but not written to.
None	Workspace cannot be read, written to, or mounted.

By default, new client accounts do not have access privileges until an administrator assigns them (see [“Adding Users” on page 93](#)). You can customize access for each client to every Workspace, if necessary.

For example, you might need to increase the access privileges for a user who does not have write access to the appropriate Workspace, or for a Workspace that does not provide the appropriate access to one or more users. To do so, you can either modify an individual client’s access privileges in the Users dialog box (see [“Modifying Users” on page 94](#)), or you can use the Workspace dialog box (see [“Setting Workspace Access Privileges” on page 81](#)).

You also can assign users access privileges different from those originally assigned to the group. If a user group is given a more permissive level of access than some members of the group, the group members then can have an effective access different from their assigned access. This can be useful for projects that require users with a variety of permissions to be able to write to certain Workspaces. You can also have users who have more permissive access than a user group in which they are members. Using the Workspaces page, the administrator can assign the necessary privileges.

Consider the following for access privileges:

- As access privileges are increased, the newly accessible Workspaces are immediately available.
- If a client has Read privileges to a Workspace and is granted Read/Write privileges, the new privileges apply immediately, without modifying the Workspace.
- If a client is already at the Workspace selection stage when the access privileges are removed, then newly inaccessible Workspaces remain in the display. However, attempting to access the Workspaces will be unsuccessful.
- If a client has Read/Write privileges to a Workspace and access privileges are reduced to read, the new privileges apply immediately, without modifying the Workspace. If a file is open for writing, the client retains write privilege to that file until it is closed.
- If a client has privileges to a Workspace and those privileges are reduced to None, then the Workspace is unavailable the next time the client attempts to access it.

Setting Workspace Access Privileges

You can set access privileges for users and user groups when the client accounts are first created (see [“Adding Users” on page 93](#) and [“Adding User Groups” on page 98](#)). You can also change access in the Users dialog box (see [“Modifying Users” on page 94](#)). The Workspaces page, however, allows you to set, modify, and monitor access privileges to Workspaces without having to modify individual client accounts.

To set user or user group access to a Workspace:

1. From the Management Console home page, click Workspaces in the System section.
The Workspaces page opens.
2. In the Workspaces list, select a Workspace.
3. If the Details panel is not visible, do one of the following:
 - ▶ Click Details.
 - ▶ Double-click the Workspace name.
 The Workspaces Details panel displays all the information on the selected Workspace.
4. In the User Access panel, select a user or a user group. Ctrl+click (Windows and Linux) or Cmd+click (Macintosh) to select multiple users and user groups. You can select all users and user groups by clicking Select All.
5. Do one of the following:
 - ▶ Click Read/Write to set both read and write Workspace access for the client.
 - ▶ Click Read to set read-only Workspace access for the client.
 - ▶ Click None to remove Workspace access privileges for the client.
6. (Option) Click Revert to undo any modifications made to the user access information.
7. Click Apply.

Redistributing Data

Redistribution is an operation that ensures all files on a Workspace are balanced evenly across the Storage Managers in the Storage Group to provide optimal file system performance. Data chunks are distributed across multiple Storage Managers to ensure redundancy and protect against data loss. When redistributing files in a Storage Group, the redistribution applies to all Workspaces in that Storage Group.

There are several operations that involve redistribution of data:

- Adding or removing Storage Managers from a Storage Group
- Deleting or moving Workspaces
- Switching Workspaces between Mirrored protection and Unprotected

Configuration Changes

The configuration of a Storage Group is based on the Storage Managers that make up that group. When you add or remove Storage Managers from the Storage Group two things happen: a configuration change is made and an incremental redistribution is performed to balance the files in the Storage Group across the Storage Managers. Deleting and moving Workspaces result in a redistribution but do not cause a configuration change. You can view the number of configuration changes that have been applied to a Workspace in the Details panel of the Workspaces page. For more information, see [“Viewing Workspace Details” on page 73](#).

After 20 configuration changes, the Workspaces page displays a warning to perform a full redistribution. You can manually initiate a Full Redistribution at any time using the Workspaces page in the Management Console. If you do not do so, the system continues to function, but the affected Workspaces, and System Status Panel general status will both remain at Warning until a full redistribution is performed. For more information on performing a full redistribution, see [“Performing a Full Redistribution” on page 84](#).



After 30 configuration changes without a full redistribution, the system will perform a full redistribution automatically. This could significantly reduce system performance until the redistribution operation has completed.

Redistribution Guidelines

- The ISIS | 7500 and ISIS | 5500 support add, remove, and full redistributions under *load*.
- The ISIS | 2500 supports add redistributions under *load*.
 - A load condition exists when the Workspace has active clients (reading and writing to the Workspace).
 - A no load condition exists when a Workspace has inactive clients (the Workspace is mounted but clients are not performing reads or writes).
- ISIS | 2500 systems do not support “remove” or “full” redistribution of Storage Managers (Engines) to a Storage Group.
- When redistributing under load, allow the redistribution to complete before initiating a second redistribution.
- System performance can degrade significantly during redistribution in a Storage Group with the maximum client count. Reducing the number of clients allows the active clients using the Storage Group to function normally, with successful playback and captures. Perform redistributions during periods of light client activity, or reduce the overall load if client performance degrades (for example, the client experiences dropped frames, underruns, and failed captures). Limitations on expected client performance during redistribution include the following:
 - Reducing audio tracks from 8 to 4 during playback might be required during redistribution. (Normal operation supports 2 streams of video 8 tracks of audio.)
 - Reducing the number of video streams from 2 to 1 might be required during redistribution. (Normal operation supports 2 streams of video.)

You can suspend and resume a redistribution as needed. See the *Avid ISIS Performance Guide* for more information.

- The amount of time a redistribution takes depends on whether the Workspace is in a load or a no load condition, whether you are adding or removing a Storage Manager, and how much data in the Storage Group must be redistributed. For more information on redistribution times, see the *Avid ISIS Performance Guide*.
- Do not physically remove a Storage Manager until it has been removed from the Storage Group, the redistribution is complete, and it has been unbound as a Storage Manager.



If you physically remove a Storage Manager from the shared storage network before redistribution is complete, or if you physically remove more than one Storage Manager from a Storage Group before performing a redistribution, data loss can occur.



If you turn off any of the Engines before redistribution is complete, data loss can occur.

Symmetric Configuration Redistribution

Full redistributions happen faster on workspaces that have had symmetric configuration changes. For example, the same number of ISBs that were removed from a storage group are also added in a single configuration change. For more examples of symmetric configuration changes search the Avid Knowledge Base for the *Avid ISIS Performance and Redistribution Guide*. As with all full redistributions, all workspaces in the storage group should be selected for the full redistribution.

A full redistribution is still recommended at 20 configuration changes. At 30 configuration changes the Avid ISIS software automatically performs a full redistribution.

Automatic Redistribution on Disk Failure

Avid ISIS performs an automatic redistribution on Disk Failure notification. Storage Managers continuously monitor disk status and sends a “Disk Failed” notification to the System Director upon determination that a disk is not usable. The System Director then removes the Storage Manager from its associated Storage Group. The removal of the Storage Manager from the Storage Group initiates redistributions on all workspaces associated with that Storage Group. The System Director then prevents the Storage Manager that reported the disk failure from being added to a Storage Group.

The Automatic Removal feature is controlled by a system preference that is configured using the ISIS Management Console Preferences tool. The preference is called “Auto Remove Redistribution on Disk Failure” The default setting is “enabled.” The Storage Manager is only removed from the Storage Group. It is not unbound from the ISIS Systems for the following reasons:

- The Storage Manager participates in the removal redistribution. This is required to prevent data loss when full redundancy has not been attained for all data blocks.
- The Storage Manager continues to report status, such as physically replacing the blade.

Auto removal status is reported by way of the System Event Log. A sequence of event log entries are generated for the initial report of the failure, the decision to remove the Storage Manager, and subsequent success or failure. Events are also logged for the start and stop of all the workspace redistributions.

When using Automatic Redistribution:

- Keep a certain percentage of your Storage Group unused at all times. Failure to do so can cause the system to run out of space after an automatic redistribution has initiated and cause a client outage. The recommended amount of free space varies by ISIS platform; for more information, see [“Minimum Free Storage Space Requirement” on page 69](#).
- If an automatic redistribution of a Storage Group is started during a critical time the overall system performance can degrade significantly and be disruptive. For more information on understanding the performance characteristics during remove redistribution, see the *Avid ISIS Performance and Redistribution Guide*.
- An automatic redistribution removes the Storage Manager from the Storage Group but not from the file system. Once an automatic redistribution has occurred and completed, the removed Storage Manager should be removed from the file system. You must first remove the Storage Manager with the software and then physically replace it. A replacement ISB must then be added to the file system and then the Storage Group, triggering another redistribution.
- If unmirrored workspaces are in use, the data will be damaged on those workspaces in that Storage Group.

Workspace Redistribution Batching

Redistributions are performed on 20 Workspaces at a time. If your Storage Group exceeds 20 Workspaces, the Workspace Status shows “Redistribution In Process” for the first 20 Workspaces and “Redistribution Pending” for the remainder of Workspaces in that Storage Group. As Workspaces finish with the redistribution, the “Redistribution Pending” Workspaces start to redistribute until all the Workspaces in that Storage Group have finished the redistribution.

Performing a Full Redistribution

In addition to automatic redistribution operations (see [“Redistributing Data” on page 81](#)), you can also initiate redistribution manually; for example, to perform a full redistribution when the Config Changes count exceeds 20. (For information about Config Changes, see [“Viewing Workspace Details” on page 73](#).)



When the Config Changes count reaches 20, a message warns you to perform a redistribution.

When redistributing files manually, apply the redistribution to all Workspaces in a Storage Group. Avid does not recommend performing a full redistribution on some Workspaces in a Storage Group and not on others.

You can choose specific Workspaces to redistribute, or select one or more Workspaces from one or more Storage Groups, and redistribute all the Workspaces associated with those Storage Groups.

To redistribute Workspaces manually:

1. From the Management Console home page, click Workspaces in the System section.

The Workspaces page opens.

2. Do one of the following:

- ▶ Select specific Workspaces, then click Advanced Commands.
- ▶ Select a single Workspace, then click Advanced Commands.
- ▶ Select one or more Workspaces from different Storage Groups, then click Advanced Commands.

The Advanced Workspace Commands dialog box opens.

3. Do one of the following:

- ▶ Click Full Redistribution.
- ▶ Click Full Redistribution for All.

Only the selected Workspaces start redistribution.
Redistribution starts for all Workspaces associated with the Storage Groups of the Workspaces you selected.

A confirmation message box opens.

4. Click OK.

Files are redistributed, and the count in the Config Changes column is reset to zero. The amount of time required for the redistribution depends on the amount of data in the Workspace.

5. If Storage Managers have rebooted following the completion of a full redistribution, do the following:

- a. Click Advanced Commands.

The Advanced Workspace Commands dialog box opens.

- b. Select Verify Redistribution, and then click Send.

Suspending and Resuming Redistribution

Under some conditions, you might have to suspend or resume an in-progress redistribution. You can do this with the Advanced Commands options available on the toolbar in the Workspaces page, which also lets you suspend or resume redistribution of all Workspaces associated with the same Storage Groups.



To suspend the redistribution on a Storage Group that has more than 20 Workspaces, suspend all the workspaces in that group.



Use of the Resume Redistribution and the Suspend Redistribution options can result in degraded system performance. Suspending redistributions can have serious consequences for the file system if not monitored closely. These two Advanced Commands options should be used by Avid Customer Support personnel or under Avid Customer Support direction.

You can also use the Advanced Commands to verify a redistribution. Verification makes sure that all bad blocks on the appropriate Storage Manager have been deleted and that the redistribution has completed successfully. Use the Verify Redistribution command whenever Storage Managers are rebooted following a redistribution — for example, after you upgrade your system. In this case, Storage Managers might report a “Repairing Mirrors” status on reboot; verifying the redistribution replays the redistribution operation using the current configuration and restores the status to normal.



Verification causes minimal impact on performance and completes quickly.

To suspend a redistribution:

1. Open the ISIS Management Console. (For information on opening the ISIS Management Console, see [“Opening the Management Console” on page 15.](#))

2. Click Workspaces in the System Area.

The Workspaces page opens.

3. Do one of the following:

- ▶ Select specific Workspaces, then click Advanced Commands.
- ▶ Select a single Workspace, then click Advanced Commands.
- ▶ Select one or more Workspaces from different Storage Groups, then click Advanced Commands.

The Advanced Workspace Commands dialog box opens.

4. Do one of the following:

- ▶ Click Suspend Redistribution.
- ▶ Click Suspend Redistribution for All.

Only the selected Workspaces suspend redistribution.
Redistribution is suspended for all Workspaces associated with the Storage Groups of the Workspaces you selected.

A confirmation message box opens.

5. Click Send.



When you manually suspend a redistribution, you must also manually resume it. Suspending redistributions should be considered temporary — Workspaces should not be left in the suspended state for extended periods of time.

To resume a redistribution:

1. Open the ISIS Management Console. (For information on opening the ISIS Management Console, see [“Opening the Management Console” on page 15.](#))
2. Click Workspaces in the System Area.
The Workspaces page opens.
3. Do one of the following:
 - ▶ Select specific Workspaces with suspended redistribution, then click Advanced Commands.
 - ▶ Select a single Workspace, then click Advanced Commands.
 - ▶ Select one or more Workspaces from different Storage Groups, then click Advanced Commands.
 The Advanced Workspace Commands dialog box opens.
4. Do one of the following:
 - ▶ Click Resume Redistribution.
Only the selected Workspaces resume redistribution.
 - ▶ Click Resume Redistribution for All.
Redistribution is resumed for all Workspaces associated with the Storage Groups of the Workspaces you selected.
 A confirmation message box opens.
5. Click Send.

To verify a redistribution:

1. Open the ISIS Management Console. (For information on opening the ISIS Management Console, see [“Opening the Management Console” on page 15.](#))
2. Click Workspaces in the System Area.
The Workspaces page opens.
3. Select the Workspace where the redistribution has completed.
4. Click Advanced Commands.
The Advanced Workspace Commands dialog box opens.
5. Select Verify Redistribution.
6. Click Send.

Redistribution Status Definitions

The following table lists the Status Messages logged by the System Director Service during a redistribution, and a brief description of the error. Other Storage Manager errors, not strictly related to redistribution, can also occur, interrupting redistribution or causing it to fail. See [“Storage Manager Status” on page 36.](#)

Status	Severity	ISIS Model	Comments
Initializing Redistribution	Warning	All	The Storage Manager is in the first phase of the redistribution process, in which it determines which blocks will be moved. The redistribution status is displayed in the Redistribution Monitor page.

Status	Severity	ISIS Model	Comments (Continued)
Redistributing	Warning	All	The Storage Manager is evenly redistributing data across all the drives in the Storage Group. The time it takes to redistribute the data depends on the amount of data in the Storage Group.
Redistribution Details Available	Warning	7500	An ISB is having trouble sending redistribution data to one or more ISBs. Do the following: • Open the ISB Storage Manager Agent page > Statistics tab > Redistribution and view the “List of Storage Managers with Transaction Issues” for problematic ISBs. • Open the ISB Storage Manager Agent page > Statistics tab > Network and view the “Top 16 IP Addresses in Receive Error (Last 30 Minutes)” section.
Stalled Redistribution	Warning	All	The Storage Manager is currently stalled while trying to move blocks to other Storage Managers. This might be a temporary condition; if it persists and the overall redistribution has been determined to be stalled contact Avid Customer Support.

Monitoring Redistributions

You can display detailed information about the progress of redistributions in the Redistribution Monitor tool.

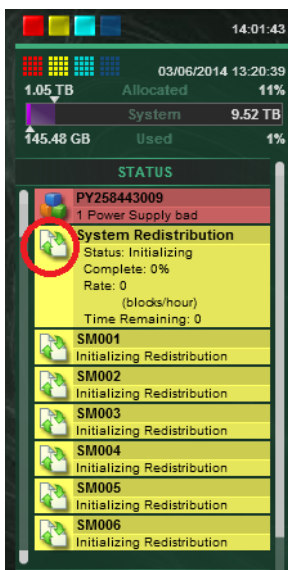
The Redistribution Monitor tool displays a table listing the status of redistributions, the rate and remaining time of the redistribution, and other information.

To display details about redistribution:

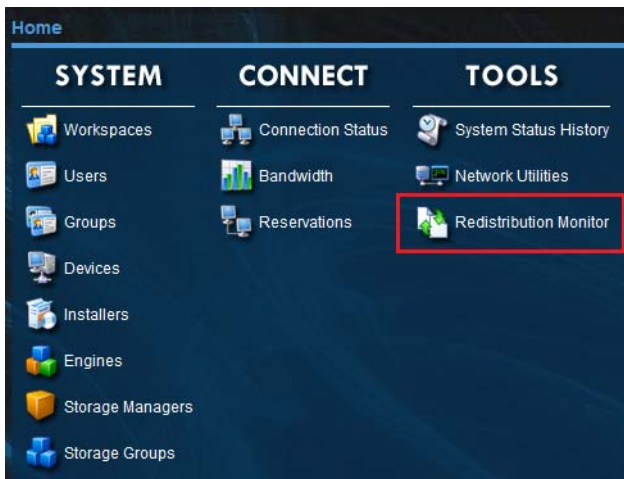
1. Do one of the following:



- If a redistribution is in process, click the Redistribution Monitor icon in the Status console.

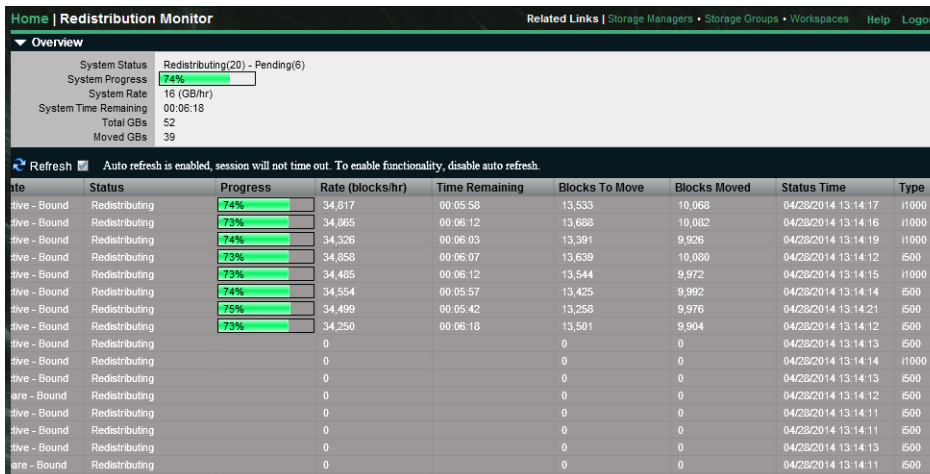


- In the Management Console, click Redistribution Monitor under the Tools heading.



- From the Workspaces tool, the Storage Managers tool, or the Storage Groups tool, click Redistribution Monitor in the Related Links section.

The Redistribution Monitor tool opens, displaying the information shown and described below.



Heading	Description
Name	Storage Manager name
ISB Name or Host Name	Name of the ISB Engine (ISIS 7500) or the host name of the Storage Manager (ISIS 2500 and ISIS 5500)
State	The state of the Storage Manager (Active or Standby, bound or spare)
Status	Redistribution status
Progress	When a redistribution is in progress, displays a progress bar and the percentage of redistribution currently complete.
Rate (blocks/hour)	Estimated number of blocks that can be moved in one hour
Time Remaining	Estimated amount of time for the redistribution to complete, based on system load, amount of data, and the rate. This is not a guarantee or promise of how long the redistribution will take.

Heading (Continued)	Description (Continued)
Blocks to Move	Total number of blocks still to be moved
Blocks Moved	Number of blocks that have been moved so far
Status Time	Time that the last status data was retrieved
Type	Storage Manager type (ISB size, ISIS Engine, Nearline Engine)

6 Managing Clients

Client accounts limit access to the file system. This section describes how to assign client accounts with associated passwords and access privileges for users, groups, and devices.

You must create a client account for any client that needs to access the Avid ISIS shared storage network: users, groups, and devices. When you create client accounts, you set basic client information, such as user names and passwords.

Each user and user group account has an associated privilege level that determines what access the user logging in to that account has when working with files stored in the network.

The ISIS Management Console allows the administrator to create client accounts for each client connected to the system, and it maintains a record of all attached clients. The client accounts are listed in dialog boxes for each client type: users, groups, and devices.

The client limits by ISIS model are as follows:

- ISIS | 7500—330 connected clients maximum
- ISIS | 5500—90 connected clients maximum
- ISIS | 2500—200 ISIS clients and unlimited CIFS clients

ISIS systems support a maximum of 5,000 user accounts (including the default Administrator and Guest user accounts). In addition, ISIS systems support 1,000 groups. A single user can be in one primary group and up to 15 alternate groups.



Some clients might not be able to connect to the shared storage network if the combined bandwidth requirement of connected components equals the system limit for bandwidth use. For information on monitoring bandwidth use, see “Monitoring Client Bandwidth” on page 110.

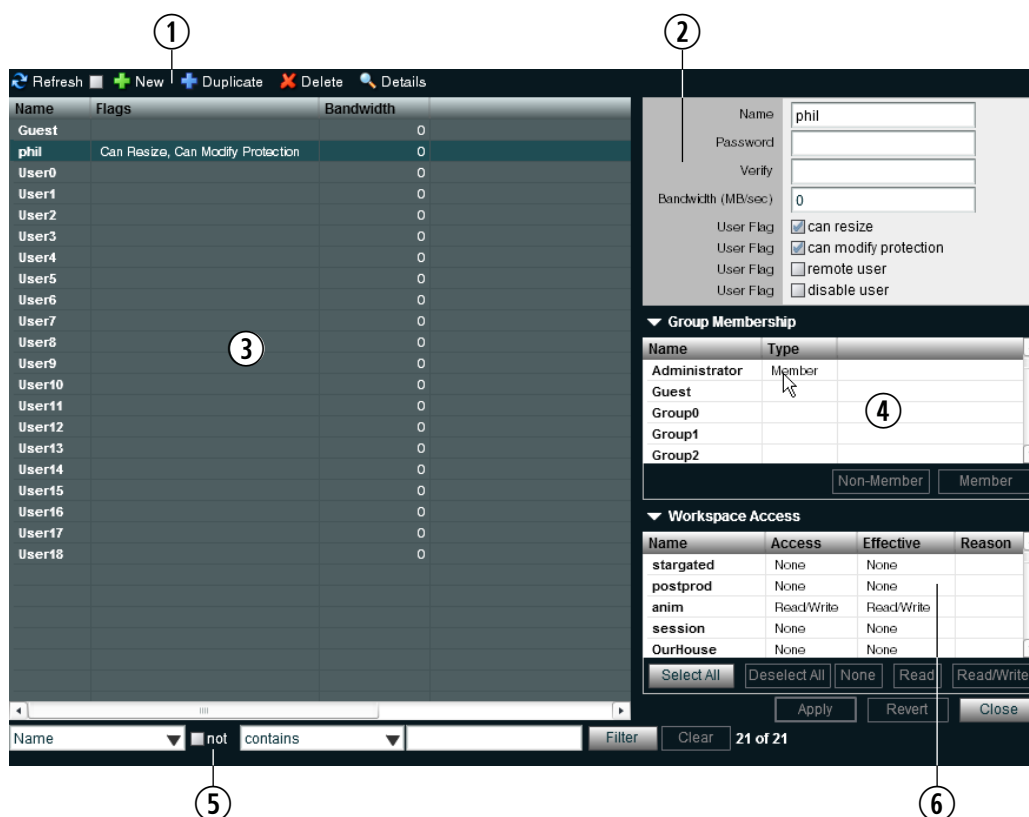
Managing Users

The Users page of the ISIS Management Console allows you to create, modify, and delete user accounts; assign users to specific groups; and manage access privileges for all users.

The Users page contains two sections. On the left side of the dialog box, the Users list displays all the current user accounts. On the right side of the dialog box, the Details panel displays information about selected users, including user group membership and Workspace access.



The Details panel is visible only after you select a client in the Users list.



- 1 Action button toolbar—Perform actions on selected users
- 2 Details panel—Detailed information on the selected users; see [“Viewing User Details” on page 92](#)
- 3 User list—Lists all users and related information; see [“User Column List” on page 91](#)
- 4 Group membership—Displays information about the group membership for the selected user; see [“Adding Users” on page 93](#) and [“Modifying Users” on page 94](#)
- 5 Filter panel—Filter the user list display based on conditions you configure; see [“Filtering the Display” on page 24](#)
- 6 Workspace access—Displays information about the Workspace access for the selected user; see [“Adding Users” on page 93](#) and [“Modifying Users” on page 94](#)

User Column List

The following table summarizes the information available in the Users list.

Heading	Description
Name	Lists the client name
Flags	Indicates the status of client privileges
Bandwidth	Lists the client’s bandwidth allocation Setting a bandwidth limit on editing clients, such as an Avid NewsCutter® Adrenaline client, can adversely affect playback performance when the Avid ISIS system is under load.



To sort the information in the Users panel, click any column heading. For more information on sorting items in columns, see “Sorting Information” on page 24.

Viewing User Details

The Details panel displays all information for the currently selected user.

To view information about a user:

- ▶ In the User list, click to select a user.

The Users page displays all the information for the selected user. If the Details panel is not visible, click Details.

To hide the User Details panel:

- ▶ Click the arrow next to the Details title bar.

To close the User Details panel:

- ▶ Click Close.

The following table summarizes the information available in the Details panel.

Panel	Heading	Description
Details	Name	Lists the user name
	Password	Allows modification of the password used to log in to the system
	Verify	Provides verification for the new password
	Bandwidth	Allows modification of maximum bandwidth requirements Setting a bandwidth limit on editing clients, such as an Avid NewsCutter Adrenaline client, can adversely affect playback performance when the Avid ISIS system is under load.
User Flag	can resize	Enables or disables user privilege for resizing Workspaces
	can modify protection	Enables or disables user privilege for changing protection status of Workspaces
	remote LDAP user	Enables or disables user LDAP authentication and group privileges
	disable user	Disables the user
Group Membership	Name	Lists the names of available groups
	Type	Lists the user’s membership status for each group (Member or Non-Member)
Workspace Access	Name	Lists the names of available Workspaces
	Access	Lists the access privileges for the selected user

Panel	Heading	Description (Continued)
	Effective	Lists the effective access privileges for the selected user
	Reason	Lists the reason for any difference between the access privileges and the effective access assigned the selected user

Adding Users

A user is anyone who accesses files stored on the network. User accounts include administrative privilege levels, group membership types, and Workspace access. There can be more user accounts than connected clients, with a maximum of 5,000 user accounts (including the default Administrator and Guest accounts).



Users must have access to at least one Workspace before they can use the shared storage network.

To create a user account:

1. From the Management Console home page, click Users in the System section.

The Users page opens.

2. Click New.

The Create User dialog box opens.

3. Set the user options. The following table summarizes these options.

Option	Type	Description
Name	text	If there is already a user with the name entered in the Name text box, an error message tells you to type a new name  <i>For information on valid and invalid characters, see “Entering Text” on page 26.</i>
Password	text	User password (maximum of 15 characters)
Verify	text	Re-type the user password to verify
Bandwidth (MB/sec)	text (numeric)	Sets a bandwidth limit for the client. The default value of zero denotes unlimited bandwidth
can resize	check box	Enables or disables user privilege for resizing Workspaces
can modify protection	check box	Enables or disables user privileges for changing protection status of Workspaces.
remote LDAP user	check box	Enables or disables user LDAP authentication and group privileges
disable user	check box	Disables the user

4. (Option) In the Group Membership list, select a group, and click Member to make the user a member in the group. Users can belong to 15 groups.

By default, new users are listed as “Non-Member” in the Type category for each group. As a result, the Non-Member button is inactive until membership is set.

The Group Membership list updates to show the user as a member of the group.

5. (Option) In the Workspace Access list, select one or more Workspaces and do one of the following:

- Click Read to set read-only Workspace access for the user.

By default, access privileges for new users are listed as “None” in the Access category for each Workspace. As a result, the None button is inactive until access is set. (For information on permissions for Workspace access in the network, see [“Managing Workspace Access Privileges” on page 80.](#))

- ▶ Click Read/Write to set both read and write Workspace access for the user.

The Workspace Access list updates to show the user access privileges for the selected Workspace.

6. Click Apply.
7. (Option) Repeat steps 3 through 6 to create new users.
8. Click Close to close the Create User dialog box and to return to the Users page.

The new user appears in the Users list.

Duplicating Users

When you duplicate user accounts, they inherit the bandwidth allocation and access privileges of the accounts from which they were created.

To duplicate a user account:

1. In the Users list, select the user account you want to duplicate.
2. Click Duplicate.

The Duplicate User dialog box opens.

3. (Option) Modify any of the attributes of the new user. For information on modifying user accounts, see [“Modifying Users” on page 94.](#)
4. Click Apply to create a new user containing the attributes of the selected user.

The duplicate user appears in the Users page, and the Duplicate User dialog box refreshes to allow you to duplicate a new user.

The new user account has a default name — user n , where n is an integer that is incremented each time you click Apply to create another duplicate user account.

5. Click Close to close the Duplicate User dialog box and to return to the Users page.

Modifying Users

You can rename a User account, change the password, change the allocated bandwidth, edit privileges, and change user membership in groups with the client dialog boxes. For example, you can change user passwords to accommodate a new user, reestablish access for an existing user who has forgotten the password, or disable access to an account.

You can modify a User account at any time, even when it is being actively used in your work environment.

To modify a User account:

1. From the User list, do one of the following:
 - ▶ Select the User account you want to modify, and click Details.
 - ▶ Double-click the client name.

The Details panel displays information about the selected User account.

2. Modify the user options as required. The following table summarizes these options.

Option	Type	Description
Name	text	If there is already a user with the name entered in the Name text box, an error message tells you to type a new name  <i>For information on valid and invalid characters, see “Entering Text” on page 26.</i>
Password	text	User password (maximum of 15 characters)
Verify	text	Re-type the user password to verify
Bandwidth (MB/sec)	text (numeric)	Sets a bandwidth limit for the client. The default value of zero denotes unlimited bandwidth
can resize	check box	Enables or disables user privilege for resizing Workspaces
can modify protection	check box	Enables or disables user privileges for changing protection status of Workspaces
remote LDAP user	check box	Enables or disables user LDAP authentication and group privileges
disable user	check box	Disables the user

3. Modify Group membership for the user as required:

- ▶ Click Member to make the user a member in the user group.
- ▶ Click Non-Member to remove the user from the user group.

4. Modify Workspace access for the user as required:

- ▶ Click None to remove Workspace access privileges for the client.
- ▶ Click Read to set read-only Workspace access for the client.
- ▶ Click Read/Write to set both read and write Workspace access for the client.

For information on permissions for Workspace access in the network, see “[Managing Workspace Access Privileges](#)” on page 80 and “[Setting Workspace Access Privileges](#)” on page 81.

5. (Option) Click Revert to undo any modifications made to the client information.

6. Click Apply.

Deleting Users

You can use the ISIS Management Console to delete any User account. If you want to remove the client from the shared storage network but still maintain the client account, see “[Disabling Users](#)” on page 96.



If you delete the client account, its connection to the System Director is broken immediately and any mounted Workspaces are unmounted as soon as they are accessed.

To delete a User account:

1. Ensure that the client account to be deleted is not currently active.
2. From the Users list, select the User account you want to delete.
3. Click Delete.

A dialog box opens, prompting you to confirm that you really want to delete the client.

4. Click OK.

Disabling Users

You can remove Users temporarily from the Avid ISIS shared storage network by using the Disable User option. Disabling User accounts do not delete them from the list of Users in the Users page. This preserves the client accounts and allows you to return the clients to the system by enabling the User account at a later time.

To remove a user by disabling the user account:

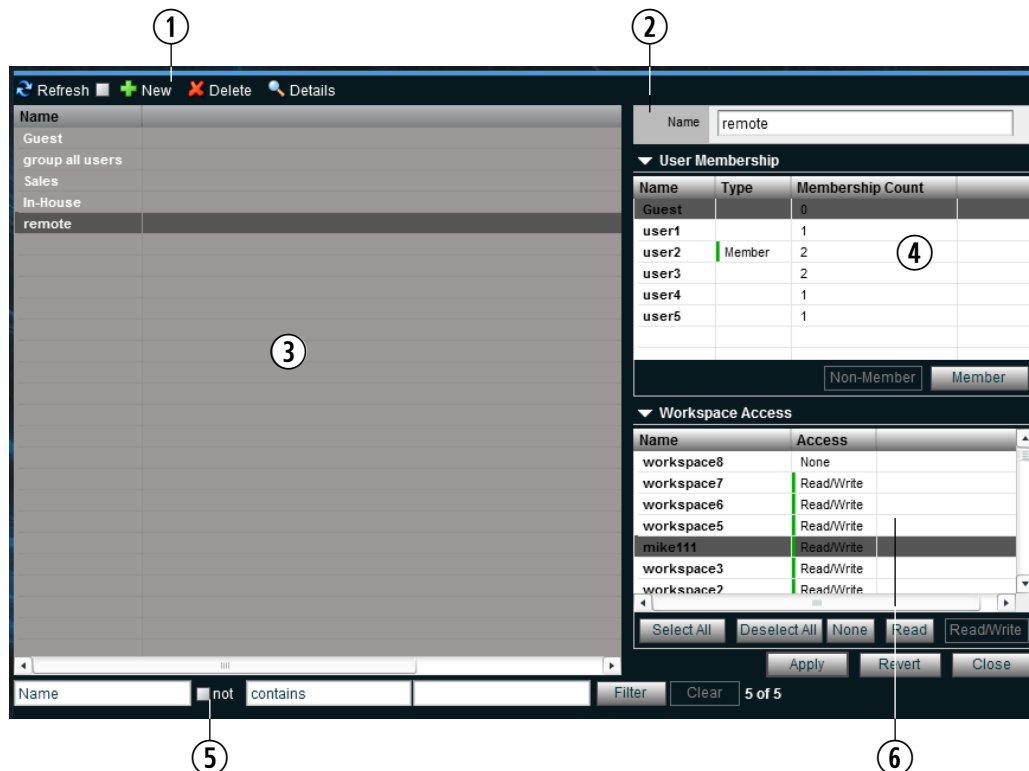
1. Ensure that the client account to be removed is not currently active.
2. From the Users list, select the client account you want to disable.
3. Do one of the following:
 - ▶ Click Details.
 - ▶ Double-click the client name.

The Details panel displays information about the selected client.

4. Select the “disable user” check box.
5. (Option) Click Revert to undo any modifications made to the client information.
6. Click Apply.
7. Click Close to close the Details window.

Managing User Groups

Client accounts also allow groups of users to access media stored on your network. These accounts allow users to mount or map Workspaces on their Avid workstations.



1	Action button toolbar—Perform actions on selected user groups
2	Details panel—Detailed information on the selected user group; see “Viewing User Group Details” on page 97
3	User groups list—Lists all user groups and related information
4	User membership panel—Displays information about the membership for the selected user group; see “Adding User Groups” on page 98 and “Modifying User Groups” on page 98
5	Filter panel—Filter the user list display based on conditions you configure; see “Filtering the Display” on page 24
6	Workspace access panel—Displays information about the Workspace access for the selected user group; see “Adding User Groups” on page 98 and “Modifying User Groups” on page 98

Viewing User Group Details

The Details panel displays all information for the currently selected user group.

To view detailed information about a User group:

- ▶ In the Group list, click to select a user group.

The Groups page displays all the information for the selected user group. If the Details panel is not visible, click Details.

To hide the User Membership or Workspace Access panel:

- ▶ Click the arrow next to the Details title bar or the User Access title bar.

To close the Details panel:

- ▶ Click Close.

The following table summarizes the information available in the Details panel.

Panel	Heading	Description
Group Details		
	<i>Name</i>	Lists the user group name
User Membership		
	<i>Name</i>	Lists the names of all users
	<i>Type</i>	Lists the user’s membership status for each user group (Member or Non-Member)
	<i>Membership Count</i>	Lists the number of groups in which each user holds membership (users can belong to no more than 15 user groups)
Workspace Access		
	<i>Name</i>	Lists the names of available Workspaces
	<i>Access</i>	Lists the access privileges for the selected user group

Adding User Groups

To add a group account:

1. From the Management Console home page, click Groups in the System section.

The Groups page opens.

2. Click New.

The Create Group dialog box opens.

3. Type a user group name in the Name text box.

If there is already a user group with the name entered in the Name text box, an error message tells you to type a new name.



For information on valid and invalid characters, see “Entering Text” on page 26.

4. (Option) In the User Membership list, select a user and click Member to make the user a member in the user group. Users can belong to no more than 15 user groups.

By default, new users are listed as “Non-Member” in the Type category for each user group. As a result, the Non-Member button is inactive until membership is set.

5. (Option) In the Workspace Access list, select a Workspace or click Select All to select all Workspaces, and do one of the following:

- ▶ Click Read to set read-only Workspace access for the user group.
- ▶ Click Read/Write to set both read and write Workspace access for the user group.

By default, access privileges for new user groups are listed as “None” in the Access category for each Workspace. As a result, the None button is inactive until access is set. (For information on permissions for Workspace access in the network, see [“Setting Workspace Access Privileges” on page 81.](#))

6. Click Apply.
7. (Option) Repeat steps 3 through 6 to create new user groups.
8. Click Close to close the Create Group dialog box and to return to the Groups dialog box.

The new user group appears in the Groups list.

Modifying User Groups

You can rename a user group account, change user membership, and modify Workspace access.

You can modify a client account at any time, even when it is being actively used in your work environment.

To modify a user group account:

1. From the Groups list, do one of the following:

- ▶ Select the user group account you want to modify, and click Details.
- ▶ Double-click the user group name.

The Details panel displays information about the selected user group account.

2. Modify the user group name as required.

If there is already a user group with the name entered in the Name text box, an error message tells you to type a new name.



For information on valid and invalid characters, see “Entering Text” on page 26.

3. Modify user membership for the user group as required:
 - ▶ Click Member to make the user a member in the user group.
 - ▶ Click Non-Member to remove the user from the user group.
4. Modify Workspace access for the user group as required:
 - ▶ Click None to remove Workspace access privileges for the user group.
 - ▶ Click Read to set read-only Workspace access for the user group.
 - ▶ Click Read/Write to set both read and write Workspace access for the user group.

For information on permissions for Workspace access in the network, see [“Managing Workspace Access Privileges” on page 80](#) and [“Setting Workspace Access Privileges” on page 81](#).
5. (Option) Click Revert to undo any modifications made to the client information.
6. Click Apply.

Deleting User Groups

You can use the ISIS Management Console to delete any user group account.

To delete a user group account:

1. Ensure that the user group account to be deleted is not currently active.
2. From the Groups list, select the user group account you want to delete.
3. Click Delete.

A dialog box opens, prompting you to confirm that you really want to delete the user group.

4. Click OK.

Managing LDAP Accounts

LDAP (Lightweight Directory Access Protocol) is an Internet protocol that some applications use to look up information — such as account information, user names, and groups — from a server. The LDAP Sync tool allows ISIS administrators to synchronize ISIS user accounts with existing LDAP user accounts and to create and/or modify a large number of users and groups within the Avid ISIS system. The LDAP Sync tool lets you:

- Display user accounts available within a given LDAP service but not in the ISIS system, and vice versa
- Add new groups and users to the ISIS system
- Grant user memberships to groups
- Remove user membership from a group in ISIS if user no longer belongs to that group on the LDAP server
- Users synchronized by the LDAP Sync tool will automatically be added as “Remote” users for authentication to the LDAP server

You can use the LDAP Sync Tool to search for groups and their users on an LDAP server, synchronize users and groups accounts by adding or removing users and/or groups from ISIS, generate a report of the account actions, and view a history of the synchronization activity. You must first configure a connection by entering the LDAP server’s fully qualified name, port, and user distinguished name and password for authentication.



Users imported by the LDAP Sync Tool cannot log into Avid ISIS server until it is configured for external authentication. For more information about configuring external authentication, see [“Configuring External Authentication” on page 30](#).



At this time, Avid ISIS currently only supports Microsoft Active Directory. ISIS might not be compatible with other LDAP implementations.

Opening LDAP Sync Tool

You can use the LDAP Sync Tool to configure LDAP connections. If you have not previously configured a connection, you must enter the connection name and other information specific to the particular LDAP server.

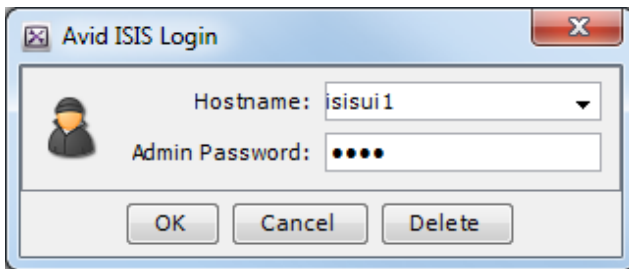


All connection information is stored locally for the connecting user's account. If you try to connect from a different workstation or as another user, you have to re-enter the ISIS and LDAP login information.

To open LDAP Sync Tool:

1. Do one of the following:
 - ▶ (Windows) From the Start menu select Avid > LDAPSynctool > Avid LDAP Sync Tool.
 - ▶ (Macintosh) Select Applications > Avid ISIS Tools > LDAP Sync Tool.

The Avid ISIS Login dialog box opens.



If the LDAP Sync tool is not installed, see “ISIS Toolbox” on page 123.

2. Type the following information in the appropriate text boxes:

Field	Value
Hostname	Fully qualified name of the LDAP server to which you are connecting
Password	Connecting user's LDAP password.



Contact your IT administrator to obtain your LDAP login information. Three failed connection attempts might result in your LDAP user account being disabled.

3. Click Connect.
 - If this is the first time using this tool, the LDAP Group Selection window opens. For more information about using the LDAP Group Selection window, see [“Synchronizing LDAP and ISIS Accounts” on page 102](#).
 - If the tool has been used before on this workstation, the main window opens.

Using LDAP Sync Tool

The Account Synchronizer is the main window of the Avid ISIS LDAP Sync Tool. Use the Account Synchronizer to search the LDAP user accounts, synchronize (reconcile) user accounts by adding or removing users from the ISIS users list, generate a report of the account actions, and view a history of the accounts. You can also modify the display of the Account Synchronizer to filter out unneeded account information.



All LDAP reconciliation session data, such as reports and history, are stored in the local user's account. If you log into another workstation and/or as a different user, this information will not be available.

When you first connect to the Avid ISIS and LDAP servers, the Account Synchronizer checks the users in the selected LDAP groups against the Avid ISIS database and builds a set of actions to reconcile the two. The main window displays the complete set of groups, using buttons with colors and icons to indicate the reconciliation status of each group.

Icon	Meaning
	The group is in the LDAP database, but not ISIS. The default action is to add the group and all users to ISIS.
	The group is in both LDAP and ISIS, but the users are different between the two: • If the user is in LDAP but not ISIS, the user will be added to ISIS. • If the user is in ISIS, but not in LDAP, the user will be removed from the group in ISIS.  <i>The user will no longer share privileges with the group. The user will still be able to access ISIS, and membership in other local or LDAP groups is unaffected.</i>
	The group is in both LDAP and ISIS, and all users are reconciled. No action is taken by default.
	The user and/or group is in ISIS, but not LDAP.  By default, all users and groups in this entry will be permanently deleted. If you do not want to remove these users from the ISIS database you must manually override the default action before performing a Reconcile action.
	The user is an ISIS only group.  By default, all users and groups in this entry will be permanently deleted. If you do not want to remove these users from the ISIS database you must manually override the default action before performing a Reconcile action.

You can click these buttons to view detailed information about actions to be performed on users in each group.

Modifying the Account Synchronizer Display

You can sort the columns in the display alphabetically, and add/remove one or more LDAP groups from the Account Synchronizer display.

To sort columns:

- Click a column heading to sort the contents of the column alphabetically. Click the heading again to reverse the sort.

To resize columns:

- Click and drag the divider between column headings.

Synchronizing LDAP and ISIS Accounts

The process of synchronizing the LDAP/Active Directory and ISIS user lists consists of the following steps:

- Selecting LDAP groups
- Specifying user-specific synchronization actions
- Performing the synchronization process



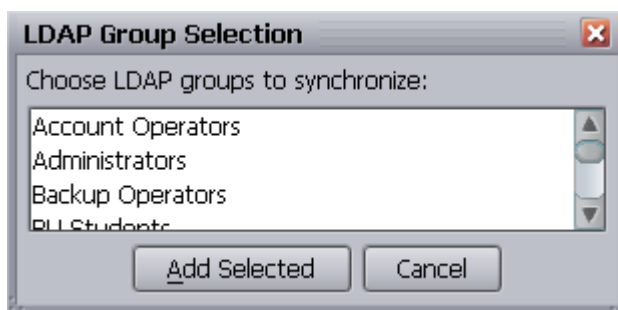
The synchronization process is read-only with regard to the LDAP/Active Directory user list. The Avid ISIS LDAP Sync Tool will never alter the LDAP/Active Directory user list.

To add groups to the Account Synchronizer display:



1. Click Select Groups.

The LDAP Group Selection window opens.



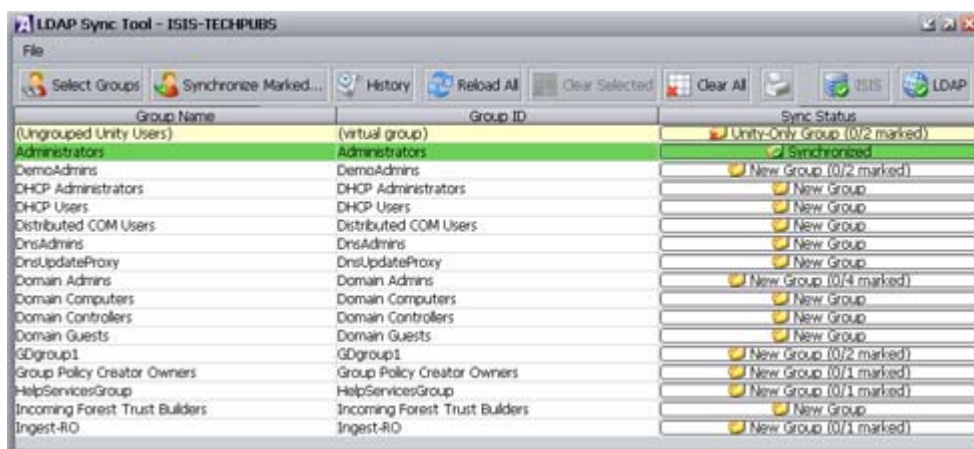
On subsequent LDAP Sync Tool sessions, the main window will open after login and display the selected groups from the last session.

2. Select the groups to be synchronized.

Selection Type	Action
Single selection	Click the group name.
Multiple non-contiguous	CTRL-click each name to be selected.
Multiple contiguous	Click the first group name, then SHIFT-click the last group name.
All	Press CTRL-A.

3. Click “Add Selected”.

The LDAP Sync Tool builds a list of sync actions for the selected groups, and displays the selected groups in the main window.



4. (Option) To print a report of the account list and selections, click Print.

To remove groups from the Account Synchronizer display:



1. Select one or more rows and click Clear Selected to remove the row from the Group list. Ctrl+click (Windows and Linux) or Cmd+click (Macintosh) or Shift+click to select multiple rows.

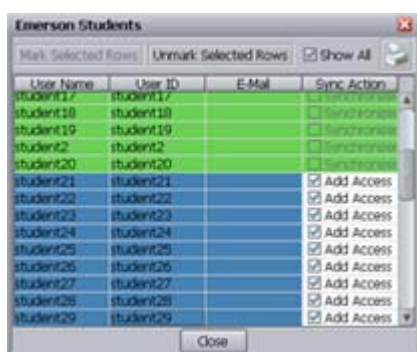


2. Click Clear All to remove all rows from the Group list.

To modify the default reconciliation actions for individual users:

1. Click the row in the Sync Status column for the appropriate group (each row in the Sync Status Column is a button).

The Descriptive name window opens and displays the user names of all members of the group, as well as actions to be taken.



2. You can do the following:

- To show all users, including those which are already reconciled, click the “Show All” check box.



The “Show All” check box is disabled if all or no users in the group are already reconciled (all users are shown by default).

- To override the default action, click the check box in the “Reconciliation Action” column to deselect it.

3. (Option) To print a report of the user list and selections, click Print.
4. Click Close to close the user selection window and return to the main window.

To synchronize LDAP/Active Directory and ISIS user databases:

- ▶ Click Synchronized Marked.

The LDAP Sync Tool performs the reconciliation actions, then displays the updated groups status in the main window.

To refresh selected entries:

1. Select one or more groups from the main window.

Selection Type	Action
Single selection	Click the group name.
Multiple non-contiguous	CTRL-click each name to be selected.
Multiple contiguous	Click the first group name, then SHIFT-click the last group name.
All	Press CTRL-A.



2. Click Reload All.

Information about the selected groups is retrieved from the LDAP server, reassessed, and displayed in the main window.

To view and/or print the History log:

1. Click History.

The History Log window opens.

2. (Option) To print the History Log, click Print.

The Print dialog opens.



3. (Option) To clear the History Log, click Delete History.

The History Log is cleared.

4. To close the History Log window, click Close.

To exit the LDAP Sync Tool

1. Do one of the following:

- ▶ Click File > Exit
- ▶ Click Close Window in the upper right corner of the window.

A confirmation window opens.

2. Click Yes.

The application closes.

Importing LDAP Users with Incorrectly Formatted LDAP UUIDs

When synchronizing users from the LDAP Synchronization Tool, the User ID (also known as the UUID) must contain characters that ISIS allows for valid user names. The entry in the User ID column is used as the ISIS Username. User names and passwords must use only ASCII characters. See [“Entering Text” on page 26](#) for more information about valid and invalid characters.

If the User ID contains any invalid characters:

- The user will not be added to ISIS
- The synchronization for the group is aborted
- Any subsequent user accounts in the group are not reconciled

In such cases, you must do one of the following:

- Create the user in ISIS with a user name that does not contain these illegal characters, and manually add them to groups.
- Update the user entry in the LDAP database with a UID that contains no illegal characters, then run the LDAP Sync Tool again to reconcile the users.

Connecting and Disconnecting from the ISIS and LDAP servers

The connection status button icons indicate whether you are connected to the ISIS and/or LDAP servers. You can use the connection status buttons to manually connect or disconnect from the LDAP server, and to reconnect with the ISIS server if the connection is lost. The button icons change depending on your current connection status.



You are disconnected from the ISIS or LDAP servers if their respective session time-out periods are exceeded.



Connected to ISIS



Disconnected from ISIS



Connected to LDAP server



Disconnected from LDAP server

To disconnect from the LDAP server:

- Click LDAP connection status.

The LDAP Sync Tool disconnects from the LDAP server, and the LDAP connection status button icon changes to Disconnected.

To connect/reconnect to the LDAP server:

1. Click LDAP connection status.

The Connect to LDAP Server window appears.



The text fields will be filled in for you if you have previously logged into the LDAP server within the same session.

2. Click Connect.

The following happens:

- The LDAP Sync Tool connects to the LDAP server.
- The Connection status icon changes to green (connected).

To reconnect to Avid ISIS:

1. Click “Connect to server” next to the ISIS server connection status icon.

The Connect to ISIS Server window opens.

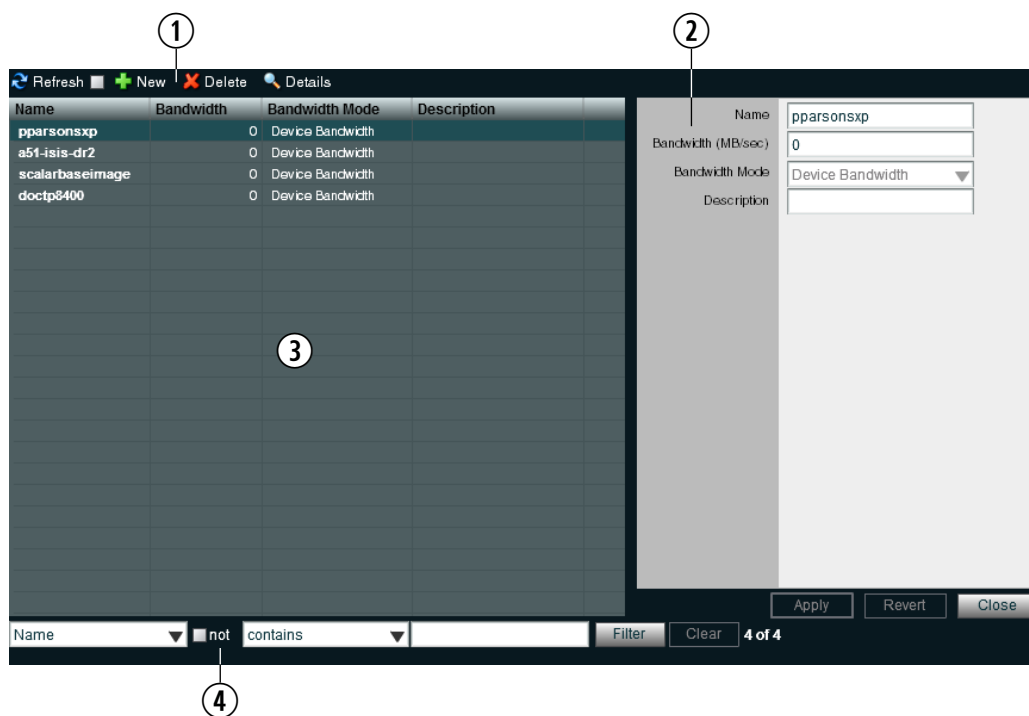
2. Enter your password into the Password text box if needed, and click Connect.

The following happens:

- The LDAP Sync Tool connects to the ISIS server.
- The Connection status icon changes to green (connected).

Managing Devices

Devices, such as Avid AirSpeed® servers, can be assigned their own client accounts. Users of the devices can then access Workspaces on the network.



-
- 1 Action button toolbar—Perform actions on selected client devices
 - 2 Details panel—Detailed information on the selected client devices; see [“Viewing Device Details” on page 107](#)
 - 3 Devices list—Lists all client devices and related information; see [“Devices Column List” on page 107](#)
 - 4 Filter panel—Filter the user list display based on conditions you configure; see [“Filtering the Display” on page 24](#)
-



If you select the Force Manual Device Creation option in the Preferences dialog box, clients who do not have an entry in the Devices list are not allowed to connect. You must manually create a device account for every client computer that is expected to connect to the ISIS system. If users deselect the Force Manual Device Creation, a client account is automatically created for each new device when it is first connected to the shared storage network. For information on preferences, see [“Configuring Management Console Preferences” on page 28](#).

Devices Column List

The following table summarizes the information available in the Devices column list.

Heading	Description
Name	Lists the client name
Bandwidth	Allows modification of bandwidth requirements  <i>You might need to set a bandwidth limit for a device such as an Avid AirSpeed in the event the device is consuming more bandwidth than expected.</i>
Bandwidth Mode	Lists the mode used to allocate bandwidth
Description	Displays the user-supplied device description, if any

Viewing Device Details

The Details panel displays all information for the currently selected client device.

To view information about a client device:

- In the Devices list, click to select a device.

The Devices page displays all the information for the selected client device. If the Details panel is not visible, click Details.

The following table summarizes the information available in the Details panel.

Heading	Description
Name	Lists the device name
Bandwidth (MB/sec)	Allows modification of bandwidth requirements  <i>You might need to set a bandwidth limit for a device such as an Avid AirSpeed in the event the device is consuming more bandwidth than expected.</i>
Bandwidth Mode	Lists the mode used to allocate bandwidth
Description	Displays the user-supplied device description, if any

Adding Devices

To create a device account:

1. From the Management Console home page, click Devices in the System section.

The Device page opens.

2. Click New.

The Create Device dialog box opens.

3. Type the system name of the device you want to add in the Name text box.

If there is already a device with the name entered in the Name text box, an error message tells you to type a new name.



For information on valid and invalid characters, see “Entering Text” on page 26.

4. Type a value in the Bandwidth text box to set the amount of read/write bandwidth (in MB/s) you want to allocate to the device. A value of 0 (zero) indicates that bandwidth will not be metered
5. (Option) Type a description of the device in the Description text box.
6. Click Apply.
7. (Option) Repeat steps 3 through 6 to create new devices.
8. Click Close to close the Create Device dialog box and to return to the Users page.

The new device appears in the Users list.

Modifying Devices

You can rename a Device account, change the allocated bandwidth, and Device description.

You can modify a Device account at any time, even when it is being actively used in your work environment.

To modify a device:

1. From the Devices list, select the Device account you want to modify, and do one of the following:
 - ▶ Click Details.
 - ▶ Double-click the client name.

The Details panel displays information about the selected Device.

2. Modify the Device options as required. The following table summarizes these options.

Option	Type	Description
Name	<i>text</i>	If there is already a device with the name entered in the Name text box, an error message tells you to type a new name
Bandwidth (MB/sec)	<i>text (numeric)</i>	Sets a bandwidth limit for the client. The default value of zero denotes unlimited bandwidth
Description	<i>text</i>	Free-text description of the device, maximum of 63 characters

3. (Option) Click Revert to undo any modifications made to the Device information.
4. Click Apply.

Deleting Devices

You can use the ISIS Management Console to delete any Device account.



If you delete the Device account, its connection to the System Director is broken immediately and any mounted Workspaces are unmounted as soon as they are accessed.

To delete a Device account:

1. Ensure that the client account to be deleted is not currently active.
2. From the Devices list, select the Device account you want to delete.
3. Click Delete.

A dialog box opens, prompting you to confirm that you really want to delete the Device.

4. Click OK.

The Device account is deleted and the Device is removed from the Devices list.

7 Managing Connections

This section describes how to use the Bandwidth page to monitor bandwidth usage in the Avid ISIS shared storage network. You can also use the Bandwidth page to remove individual components from the network.

Monitoring Client Bandwidth

The Bandwidth page allows you to monitor system usage, including total system bandwidth use and bandwidth consumption of each connected system.



- 1 System bandwidth scale buttons—Increase or decrease the scale of the system bandwidth graph; see [“Scaling the Bandwidth List Graph Display” on page 111](#)
- 2 System bandwidth read and write graphs—Graphic display of system read (green) and write (red) bandwidth; see [“Bandwidth List” on page 111](#)
- 3 Device bandwidth scale buttons—Increase or decrease the scale of the device bandwidth graph; see [“Scaling the Bandwidth List Graph Display” on page 111](#)
- 4 Device bandwidth read and write graphs—Graphic display of device read (green) and write (red) bandwidth; see [“Bandwidth List” on page 111](#)

The System Read Bandwidth and System Write Bandwidth rows in the Bandwidth page show total system read bandwidth (green bar) and total system write bandwidth (red bar) in megabytes per second (MB/s).

Below the System Read Bandwidth and System Write Bandwidth rows is a list of all active system components showing their current activity and their system identification.

Opening the Bandwidth Page

To open the Bandwidth page:

- ▶ From the Management Console home page, click the Bandwidth icon, located in the Connectivity section.
The Bandwidth page opens.

Bandwidth List

The following table describes the information displayed in the Bandwidth page.

Heading	Description
System Read Bandwidth	The value of the total system bandwidth currently in use for reading files (in MB/s)
System Write Bandwidth	The value of the total system bandwidth currently in use for writing to files (in MB/s)
System Name	The name of the system specified during the System Director configuration
Read BW	For the listed system components, the value of the bandwidth currently in use for reading files (in MB/s)
Write BW	For the listed system components, the value of the bandwidth currently in use for writing to files (in MB/s)
Bandwidth	For the listed system components, graphical display of bandwidth usage: • Read (green bar) • Write (red bar)



To sort the information in the Bandwidth Monitor list, click any column heading. For more information on sorting items in columns, see “Sorting Information” on page 24.

Scaling the Bandwidth List Graph Display

The Bandwidth Monitor list represents bandwidth consumption for the network and for individual system components in the form of horizontal bars in a graph display. Numeric divisions are displayed in megabytes/second (MB/s). You can adjust the scale of the graph to make it easier to monitor bandwidth information.

To decrease or increase the size of the graph view:



- ▶ Click Decrease Size or Increase Size button.

Monitoring System Connection Status

The Connection Status page allows you to view the status of all components connected to the network. You can also use the Connection Status page to disconnect components from the system.



Some clients might not be able to connect to the shared storage network if the combined bandwidth requirement of connected components equals the system limit for bandwidth use. For information on monitoring bandwidth use, see “Monitoring Client Bandwidth” on page 110.

Refresh Disconnect					
Name	ID	Os	Type	License	Last Seen
isis-techpubs	4	vWindows	MicroServer	0	
isis-techpubs1724	2,001	vWindows	Admin	0	

- 1
- Action button toolbar—Perform actions on selected components
- 2
- Connections list—List connected components and related information; see [“Connection Status Descriptions” on page 112](#)

Opening the Connection Status Page

To open the Connection Status page:

-
- From the Management Console home page, click the Connection Status icon, located in the Connectivity section.
- The Connection Status page opens.

Connection Status Descriptions

The Connection Status dialog box lists information about all components — both active and inactive — that comprise the shared storage network. The following table describes the information displayed in the dialog box.

Heading	Description
Name	Lists the name of the component
ID	Lists an internal numeric identifier used by the System Director to represent the component; these identifiers are assigned when a component first contacts the System Director
OS	Lists the operating system of the component
Type	Lists the category or principal function of the component
License	Displays the number of licenses allotted to the component
Last Seen	For inactive components, displays the date and time when the component last sent its status to the System Director; for active components, displays a zero (0) as the default value For active components, displays the date and time when the component last sent its status to the System Director. The System Director removes information about components that have not been seen for a week, unless the component’s bandwidth limit is configured to custom values or the Default Device Bandwidth option in the Preferences dialog box is selected



To sort the information in the Connection Status dialog box, click any column heading. For more information on sorting items in columns, see “Sorting Information” on page 24.

Disconnecting Clients from the Shared Storage Network

You can use the Connection Status dialog box to momentarily disconnect clients from the shared storage network. Disconnecting clients moves them from active to inactive status in the list of active clients in the Connection Status dialog box. Inactive clients display the time of the last logged contact between the System Director and the clients.



Before disconnecting a client from the network, determine the status of active clients (for example, determine whether any clients currently have Workspaces mounted on the client you want to disconnect). For information on using the Monitor tool to determine the status of active clients, see “Managing Active Clients” on page 59.

To disconnect a client from the shared storage network:

1. Select a client from the list.
2. Click Disconnect.

A dialog box opens asking you to confirm the action.

3. Click Yes.

The changes might not appear until the list is refreshed.

Monitoring Reservations

Normally, bandwidth reservations are initiated and configured automatically by Avid applications based on bandwidth requirements. In some cases however, you might want to limit the bandwidth available to client systems. Client workstation users can use the Client Manager to obtain a default bandwidth reservation on the ISIS system. The actual bandwidth available to the client is the lowest of the following values:

- The default bandwidth requested by the Client Manager
- The maximum bandwidth assigned by the ISIS Administrator to the user
- The maximum bandwidth value assigned by the Management Console, either per-device or by the default bandwidth allocation for auto-created devices
- The bandwidth limitation of the client device

You can use the Reservations page to monitor the status of client reservations, and to revoke client reservations, if necessary.

Refresh Revoke Reservation	
System Name	Reservation
scalarbaseimage	3.75 MB

- 1 Action button toolbar—Perform actions on selected client reservations
- 2 Reservations list—List clients with reservations and related information; see [“Reservations Descriptions” on page 114](#)

Reservations Descriptions

The Reservations page lists information about all bandwidth reservations obtained by connected clients. The following table describes the information displayed.

Heading	Description
System Name	The computer name of the client system
Reservation	The value of the bandwidth reservation, in MB/sec.



To sort the information in the Reservations page, click any column heading. For more information on sorting items in columns, see [“Sorting Information” on page 24](#).

Revoking Reservations

You can revoke a client reservation using the Reservations page. Revoking a reservation will only remove the bandwidth reservation; the client will still be connected to the Workspace.

To revoke a reservation:

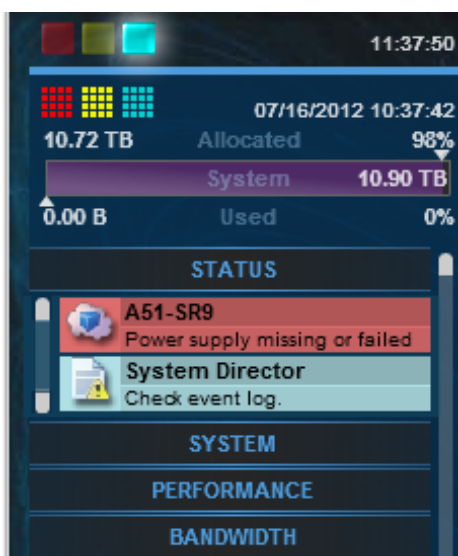
1. From the Management Console home page, click the Reservations icon, located in the Connectivity section.
The Reservations page opens.
2. Select one or more client systems for which you want to revoke the bandwidth reservation.
3. Click Revoke Reservation.
A confirmation dialog opens.
4. Click Yes.
The client reservation is revoked.

8 System Monitoring and Diagnostics

Avid ISIS Management Console provides tools for logging, monitoring, and system diagnostics.

Hardware Monitoring Service

The Hardware Monitoring service runs on all ISIS | 5500 Engines, and to a limited extent on ISIS | 2500. It periodically polls certain critical components on the Engine and reports status to the System Director. The System Director then makes this status available to the Management Console. Errors and warnings are indicated in the System Status Console. Expand the Status Console panel to view what component that is causing the error or warning.



These status messages inform you of system issues that might not be obvious because in most cases the ISIS system can continue to function. The issues should be corrected so that a more serious failure does not occur. The components and messages that are displayed in the Status Console panel are listed in the following table.

Component	Category	Message Text	Description
Power Supply	Error	Power supply missing or failed	One or more power supplies have failed, are failing, or do not have a power cable plugged in.
System RAID Volume (ISIS 5500)	Error	Storage volume missing or failed	The system RAID volume is degraded or failed (there is only <i>one</i> system volume).
Fan (ISIS 5500)	Error	Fan missing or failed	The Engine fan is missing or has failed.
Approved Network settings	Warning	Incorrect network adapter settings	One or more of the network adapters used for ISIS communication do not have the correct settings applied.

For a list of event logs generated by the Hardware Monitoring service, see [“Avid ISIS E-mail Notification List” on page 173](#).

System Information Page

You can use the System Information page of the Management Console to view basic information about your system and your network. You cannot edit the information displayed in the System Information window. Many of these items are also displayed in the Avid ISIS Launch Pad.

Category	Heading
Server Status	• Server state • Active • Server Version • Event Log Status (ISIS 7500)
Server Details	• Virtual Name • Local Host Name • Flock ID • Port Number • Licensed clients allowed • Licensed clients connected • Interface 0 through x (depends on the number of Ethernet ports in your System Director)
Metadata	• Loaded • Creation Time • In Use • Available • Available (Large Allocations) • Total • Percent Used • Verified Status • Verified Date • Saved Status • Saved Date
Dual System Director Configuration	Enabled

Category (Continued)	Heading (Continued)
Host Information	• Username (ISIS 7500, ISIS 5500) • Hostname • OS Version • Processor Type • Number of Processors • System Uptime
Memory Information	• Total Physical Memory • Total Physical Memory Usage • Available Physical Memory • Total Page File • Available Page File
Running Processes	List the processes running on the System Director
Agent Environment	• Server name • URL • GUID • Root directory • Work directory • WSDL directory • Cookie domain • Cookie path • Soap version • Soap accept timeout • Soap send timeout • Soap recv timeout • Soap max keep alive • Running interactively
Agent Statistics	• Version • Start Time • Requests • Failed soap accepts • Failed ssl accepts • Failed soap allocations • Failed thread allocations • Memory usage

Category (Continued)	Heading (Continued)
Agent Configuration	• Server listen backlog • Server accept timeout • Server failed accept limit • Server send timeout • Server recv timeout • HTTP session timeout • HTTP expires time (secs) • SSL disabled • SSL certificate file • SSL verify client • SSL ca certificate file • SSL ca certificate path • Agent network tool timeout (secs) • Agent reboot reconnect time (secs)

To view System Information:

- From the Management Console home page, click the System Information icon, located in the Logging section. The System Information page opens.

System and Administration Log Pages

The Logging window provides a complete view of the Logs of a network, including active Storage Managers, System Directors, and clients. You can filter the log reports to display messages about the network, the Avid ISIS file system, or security information. This provides you with a system snapshot that you can use to view error and status messages. The logs provide detailed status information that is especially useful to Avid Customer Support personnel for monitoring system status during prolonged operations.

Using the Administration Logs

You can view the log of the ISIS Management Console from the Administration Logs window in the Logging section of the ISIS Management Console. The log lists the actions reported by the ISIS Management Console, including informational messages (such as when upgrades occur), errors, and warnings. You can sort the log entries by column or filtered. The log lists the following data for each event:

- Type — The categories are the following: Info, Error, Warning
- Time — The time of the logged event
- IP — The recorded IP address of the client or the System Director, depending on where the logged event happened
- User — The ISIS user who initiated the event
- Message — Detailed information about the event

To view the Administration logs:

1. From the Management Console home page, click the Administration Logs icon, located in the Logging section.
The Administration Logs page opens.
2. Do one of the following:
 - ▶ Click View to view the Administration logs.
 - ▶ Click Download to download the Administration logs in Comma Separated Values (CSV) format.
3. (Option) To filter the log entries in the View Administration logs window:
 - a. Type the appropriate keyword in a Filter text box.
 - b. Press Enter. To view all log entries, clear the text box and press Enter.
4. (Option) To refine your filtering, enter keywords into multiple Filter text boxes.
5. If the log contains more entries than it displays, use the Navigation controls to move through the log.

Using the System Logs Page

System logging allows you to select the events to view by restricting the logs to the following categories:

- System — Displays events associated with system configuration
- Application — Displays events associated with the functioning of the System Director software
- Security — Displays events related to security in the network

Viewing System Logs

You can use the System Logs window to view event logs and to clear existing logs.

To access System Logging functions:

1. From the Management Console home page, click the System Logs icon, located in the Logging section.
The System Logs page opens.
2. Click Select Log to view menu, and select one of the following:
 - System
 - Application
 - Security
3. Click View.

The selected log displays in the Logs panel.

Clearing System Logs

You can clear the logs in any of the logging categories. This empties the log of all event entries and resets the logging process.

To clear logs:

1. Click Clear.
2. Click OK.

The event log for the selected category is cleared, and logging is reset to start recording new events.

ISIS Snapshots Page

The ISIS Snapshots page collects information currently displayed by the ISIS Management Console and the Avid ISIS System Director Control Panel and allows you to view and archive the information. This snapshot of your ISIS system at a single point in time, coupled with the system logs collected by the Log Aggregator tool (see [“Log Aggregator Tool” on page 125](#)), can be used by Avid Customer Support personnel to diagnose and troubleshoot problems.

The Snapshots page collects information from the following pages, dialog boxes, and tabs of the ISIS Management Console and the Control Panel:

Category	Description
General Info	Includes the System Director computer name and virtual name, the snapshot run date, and a link to the compressed snapshot file
ISIS Components	Lists the ISIS components from the Command menu of the ISIS Management Console, any warnings or errors logged, and a link to a comma separated value (CSV) file for each component containing the information displayed in the Details panel of each component page; you can open the CSV file with an appropriate text editing application
Warnings and Errors	Lists all warnings and errors currently logged for all components in the ISIS system
System Director Status	Summarizes the information on the System Director Status tab of the System Director Control Panel (for more information, see “Monitoring System Director Status” on page 55)
System Director Metadata	Summarizes the information on the Metadata Status tab of the System Director Control Panel (for more information, see “Monitoring Metadata Status” on page 57)
Dual System Director Configuration	Summarizes the information on the Dual System Director Configuration dialog box of the System Director Control Panel
Preferences	Summarizes the information on the Preferences dialog box, accessed from the ISIS Management Console (for more information, see “Configuring Management Console Preferences” on page 28)

Creating, Viewing, and Deleting Snapshots

You use the ISIS Snapshots page to create a detailed view of your system at a particular time. The snapshot is saved as a series of CSV files, one for each component in the system, and a summary file in HTML format. Snapshot files are saved in folder named by the timestamp of the snapshot and the System Director name — for example, 07-17-07 101321 AvidISIS — at the following location within the application directory:

```
D:\Program Files\Avid\ISIS System Director\webroot\snapshot
```

You can also download the snapshot in compressed form as a ZIP file by clicking Download.

To create a snapshot of the ISIS system:

1. From the Management Console home page, click the ISIS Snapshots icon, located in the Logging section.
The ISIS Snapshots page opens.
2. Click New.
3. Enter a name for the snapshot or accept the default name (default) and click OK.

The Snapshot page creates a snapshot and displays the information in the ISIS Snapshot window.

To delete a selected snapshot:

1. Select a snapshot from the list.
2. Click Delete.

A confirmation dialog window opens.

3. Click OK to confirm the deletion.

The Snapshot page deletes the selected snapshot.

To delete all snapshots:

1. Click Delete All.

A confirmation dialog window opens.

2. Click OK to confirm the deletion.

The Snapshot page deletes all snapshots listed in the System window.

Working with Snapshot Archives

When the Snapshot page creates a snapshot, it creates a folder which includes a compressed file containing all information collected by the tool. You can combine snapshots into an archive to keep track of the system status — for example, you could archive snapshots weekly or monthly. The Snapshot tool compresses archives in a ZIP file (*archivename.zip*).

Archives are stored in folders named by the timestamp of the snapshot and the System Director name — for example, 07-17-07 101321 AvidISIS. The compressed archive uses the same file name format as the snapshot folder and is saved to the following location within the application directory:

```
D:\Program Files\Avid\ISIS System Director\webroot\snapshot
```

You can also download the archive in compressed form as a ZIP file by clicking Download.

To create a snapshot archive:

1. From the ISIS Snapshots page, click New next to Archives.

A confirmation dialog window opens.

2. Click OK to confirm building a new archive from all current snapshots.

The Snapshot page creates an archive and lists it in the Archives area.

To delete a snapshot archive:

1. Select a snapshot archive you want to delete from the list. (If there are no snapshot archives, the ISIS Snapshots page displays “No Available Archives.”)
2. Click Delete.

A confirmation dialog appears.

3. Click OK to confirm the deletion.

The Snapshot page deletes the selected archive.

To delete all archives:

1. Click Delete All.

A confirmation dialog window opens.

2. Click OK to confirm the deletion.

The Snapshot page deletes all archives listed in the System window.

Profiler Page

The Profiler page detects the current versions of required software, drivers, and hardware components that are installed on a System Director. You can view, save, or delete profiles, but you cannot use the Profile page to edit or modify the information.

Profiles are typically used by Avid Customer Support to help determine problems with installed versions of the operating system, drivers, adapter boards, or firmware. Besides running the Profiler from the Management Console, you can also run Profiler by clicking Start > Programs > Avid > ISIS System Director and selecting ISIS Profiler.



The Profiler tool is also installed with the Client software and can be run on the Client by clicking Start > Programs > Avid > ISIS Client and selecting ISIS Profiler.

To create a new profile:

1. From the Management Console home page, click the Profiler icon, located in the Logging section.

The Profiler page opens.

2. Click Create New Profile.

The new profile displays in the Profiles window.

To view profiles of the local system:

1. Select the Profile you want to view from the list.
2. Click View.

The profile displays in the Profiles window.

To delete a profile from the Profile window:

1. Select the Profile you want to delete from the list.
2. Click Delete.

A confirmation dialog window opens.

3. Click OK.

To delete all Profiles:

1. Click Delete All.

A confirmation dialog window opens.

2. Click OK.

System Status History Page

You can use the System Status page to view the record of system status information collected periodically by the System Status Console.

To open the Status History page:

- From the Management Console Home page, click the System Status History icon from the Tools section.

The System Status History page opens to the day of the first logged system event.

To view information on a system event:

1. In the Hours column, click on the hour with the colored icon corresponding to the time and type of system event you want to view.

The Seconds column opens.

2. In the Seconds column click on the second with the colored icon corresponding to the time and type of system event you want to view.

A snapshot image of the System Status Console, taken at the time of the logged event, is displayed.

To clear Status History Event flag:

- Click “Clear status event history flag”.

The status event history panel indicator is cleared.



This command only clears the status event history indicator from the System Status Console. It does not remove any status event history entries.

ISIS Toolbox

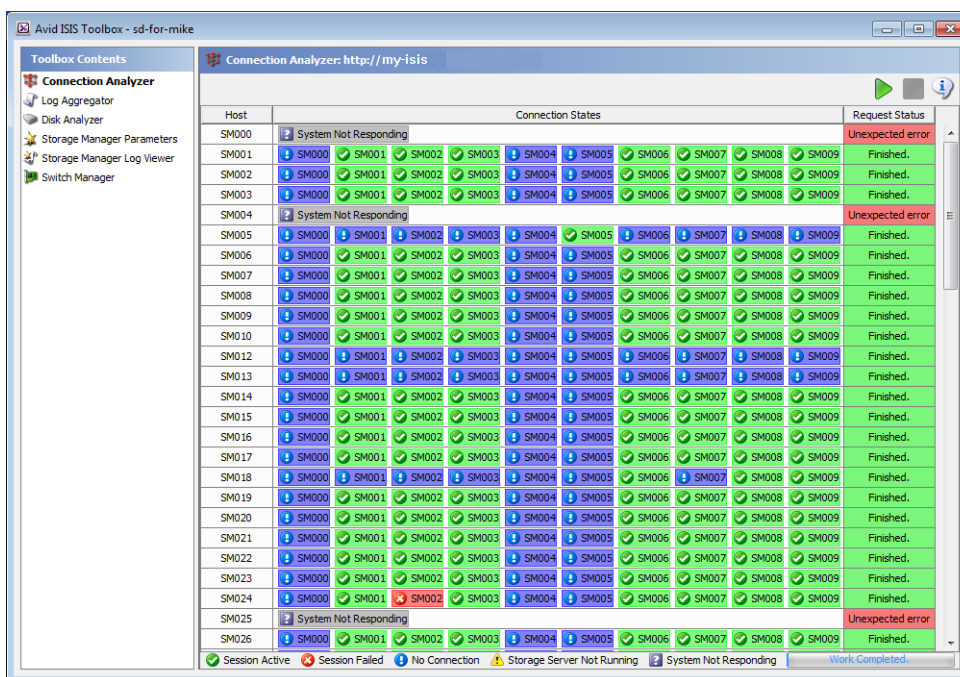
Avid ISIS Toolbox is a collection of tools you can use to monitor and perform diagnostic operations on all your ISIS hardware. Using the provided visual indicators, you can quickly narrow your search to the intended system event.

To install the Toolbox:

1. In the Management Console, click Installers under the System heading.
2. In the ISISTools section, click the Toolbox executable file appropriate for your operating system.
3. Save the executable file to your computer and install it.

Connection Analyzer Tool

The Avid ISIS Connection Analyzer provides a quick look at the connection status of all Storage Managers in the shared storage network.



The Connection Analyzer displays connection status in a grid, using the following icons to denote the status of each Storage Manager:

Icon	Label	Status
	Session Active	Source Storage Manager has a session with the target Storage Manager
	Session Failed	Source Storage Manager does not have a session with the target Storage Manager
	No Connection	Target Storage Manager is not communicating with the System Director
	Storage Server Not Running	Microserver failure—Failure in the request from the Agent to the Storage Manager for session information—for example, a failed request resulting from the Storage Manager not running or the Storage Manager not servicing the request before it timed out
	System Not Responding	Communication failure—Unable to determine status—for example, the Agent is not running or there is a network problem between the Connection Analyzer tool and the Storage Manager

To open the Connection Analyzer and test the connection status of Storage Managers:

1. Do one of the following:

- ▶ (Windows) Select Start > Avid > Toolbox > Avid ISIS Toolbox.
- ▶ (Macintosh) Select Applications > AvidISISTools > ISIS Toolbox.

If any site security warnings open, click Yes to accept the certificate. If you are not sure about the security requirements of your shared storage network, see your system administrator.

The Avid ISIS Toolbox opens.

2. Click Connection Analyzer from the left pane.

The Avid ISIS Connection Analyzer window opens and checks the connection status of all Storage Managers in the network. The tool displays results in a color-coded grid.

If you place your pointer over a block in the grid, a tooltip indicates to which Storage Managers the status applies. This is useful when you have more Storage Managers than can be displayed in the dialog box and you need to use the scroll bars to view a specific connection.



3. (Option) Click Info to display version information.

To update the status of Storage Managers:



1. Click Start to update the status of Storage Managers without reloading the entire Storage Manager list from the System Director.



2. (Option) To stop the status update operation, do the following:

- a. Click Stop.

A confirmation dialog appears.

- b. Click Yes.

The update process stops and the main display returns to the previous result.

Log Aggregator Tool

The Avid ISIS Log Aggregator tool allows you to collect a full set of the event logs and system statistics of a network, including active Storage Managers, Avid ISIS Switch Blades (ISIS | 7500), and the System Director. You can select which information—from the network, the System Director software, and Storage Managers — you want to collect in the log reports. This provides you with a system record that you can use to view error and status messages. The logs provide detailed status information that is especially useful to Avid Customer Support personnel for monitoring system status during prolonged operations.



Do not use the Avid ISIS Log Aggregator unless instructed to do so by Avid Customer Support. Improper use could result in system downtime or degraded performance.

LSI Log Aggregator

The ISIS | 5500 includes an LSI Log Aggregator tool that is set to run daily at 1:00 a.m. This tool gathers data on the LSI RAID controller. It runs for approximately for 5 minutes and does affect user performance. The log gathering option are Enabled in the Aggregation Options dialog box and are called “Engine RAID logs and Disk Config logs.”

Using the Log Aggregator Tool

The Log Aggregator lists all components of the shared storage network in a tree view. You can select events to log in two ways:

- You can view events for all components in the shared storage network by selecting all active Avid ISIS systems in the Selection window (the highest level in the tree view).
- You can view events for any subset of components by selecting one or more entries in the Selection window (at a level lower than the Avid ISIS Systems in the tree view).



You must run the Log Aggregator from a system with network access to the entire shared storage network. Otherwise, the tool cannot collect logs for all systems connected to the network.

To open the Log Aggregator tool:

1. Do one of the following:

- ▶ (Windows) Select Start > Avid > Toolbox > Avid ISIS Toolbox.

- ▶ (Macintosh) Select Applications > AvidISISTools > ISIS Toolbox.

If any site security warnings open, click Yes to accept the certificate. If you are not sure about the security requirements of your shared storage network, see your system administrator.

The Avid ISIS Toolbox opens.

2. Click Log Aggregator in the left pane.

The Log Aggregator window opens.

To close the Log Aggregator:

1. Click Close.

A dialog box opens asking you to confirm that you want to quit the ISIS Toolbox.

2. Click Yes.

Creating Aggregate Logs

To use the Log Aggregator, you must have Administrative privileges and be logged into a system with access to the shared storage network.

To create logs with the Log Aggregator tool:

1. Open the Log Aggregator tool. (For information on opening the Log Aggregator, see [“Using the Log Aggregator Tool” on page 125.](#))

2. In the Selection window, do one of the following:

- ▶ Select all active Avid ISIS systems to view events from all components in the shared storage network.
- ▶ Select one or more components to view events from specific System Directors, Storage Managers, and clients attached to the network.



3. Click Configure.

The Aggregation Options dialog box opens.

4. Configure the following options to customize the data collected in the event logs:

Option	Description
Common Aggregation Options	Types of Windows logs or information
System Director Options	Types of System Director logs or information
Storage Manager Aggregation Options	Types of Storage Manager statistics or logs
Switch Blade Aggregation Options (ISIS 7500)	Types of Storage Manager statistics or logs
Archive Options	Whether to create a compressed archive file (Log Aggregator__date-time) and whether to delete the fetched files after archive creation; the file is saved to the directory specified in the Target Directory text field in the Log Aggregator window
Concurrent Retrieval Threads	Adjust the slider to maximize the use of resources in your system when collecting logs. The default number of threads is 10. A lower number uses fewer system resources but requires more time to complete log aggregation; a higher number uses more resources but completes the operation faster

5. Click OK to close the Aggregator Options dialog box and return to the Log Aggregator.



6. (Option) In the Target Directory text section, click Browse to navigate to a directory for the saved logs.
7. Click Start.

The progress bar indicates the status of the log aggregation. The Log Aggregator displays a Success icon (green) or a Fail icon (red) for each system and component logged. You can cancel the log aggregation process by clicking Abort.

Viewing Aggregate Logs

The Log Aggregator saves individual logs in a log directory called ISISLogs__*date-time* at the location indicated in the Target Directory section in the Log Aggregator. Subdirectories include separate logs for each component in the network for which you created logs. The Log Aggregator also creates a compressed file containing all logs in the top-level folder (aggregator_results.zip). You can forward this compressed file to your Avid representative if requested by Avid Customer Support.

To view saved logs:

1. Navigate to the directory where the Log Aggregator saved the collected logs.
2. Double-click the file name of the log you want to view.

Disk Analyzer Tool

The Avid ISIS Disk Analyzer runs basic disk performance tests on your Storage Managers. The tests include the following, which you can run in either Sequential or in Random access mode:

- Read test
- Write test
- Read/Write test
- Erase test

You can also use the Disk Analyzer to collect statistics on the status of Storage Managers and network use, and redistribution actions, including the statistics generated by Self-Monitoring, Analysis, and Reporting Technology (S.M.A.R.T.—on ISIS | 7500 systems) and by local Storage Manager processes — for example, statistics on Long Command Times (LCT).



S.M.A.R.T. data is also available for ISIS | 7500 and ISIS | 2500 systems through the Log Aggregator tool.

You can run the Disk Analyzer on more than one Storage Manager at a time; however, running the tests might degrade performance on the shared storage network.



Do not run the Disk Analyzer unless instructed to do so by Avid Customer Support, and only during a maintenance window.

Opening the Disk Analyzer Tool

To open the Disk Analyzer tool:

1. Do one of the following:
 - ▶ (Windows) Select Start > Avid > Toolbox > Avid ISIS Toolbox.
 - ▶ (Macintosh) Select Applications > AvidISISTools > ISIS Toolbox.

If any site security warnings open, click Yes to accept the certificate. If you are not sure about the security requirements of your shared storage network, see your system administrator.

The Avid ISIS Toolbox opens.

2. Click Disk Analyzer from the left pane.

The Disk Analyzer window opens.

Updating the Disk Analyzer Tool Display

To update the display:



- Click Refresh.

Running Disk Analyzer Tool Tests

To run a test on the Disk Analyzer:

1. Open the Disk Analyzer.
2. Click Disk Analyzer menu and select one of the following:
 - Execute disk tests
 - Collect disk statistics
 - Collect network statistics
 - Collect redistribution statistics
3. In the Selection window, do one of the following:
 - Select all active Avid ISIS systems to test all Storage Managers in the shared storage network.
 - Select one or more Storage Managers to test specific components in the network.



4. Click Start.

If you selected Execute disk tests, the Disk Test Options dialog box opens.

5. Configure the appropriate options for the test you want to run.

Option	Description
Test Type	The type of test to be performed
Access Mode	Perform sequential or random access test
Concurrent I/Os	Number of input and output operations to run concurrently
Duration	Test duration in minutes or number of passes (specify the number of passes in the text field)
Refresh Rate	How often the test status is updated
Reattach to existing tests	By default, starting a new test will abort any currently running tests and clear any existing results. Select this option to resume any currently running tests and retain the results

6. Click OK to close the Disk Test Options dialog box and return to the Disk Analyzer.

Results of the test display in the Results area.

Saving Disk Analyzer Test Results

You can save the results of the Disk Analyzer tests to your local system. The test results are saved in comma separated value (CSV) format.

To save the results of the Disk Analyzer tests:



1. Click Save Results.

The Save Results window opens.

2. Browse to the location on your local system where you want to save the test results and click Save.

The test results are saved to the specified location.

Storage Manager Parameters Tool

The Avid ISIS Storage Manager Parameters tool allows you to set and retrieve Storage Manager logging and redistribution flags. This status information is useful to Avid Customer Support personnel for monitoring system status during prolonged operations.



Do not use the Avid ISIS Storage Manager Parameters tool unless instructed to do so by Avid Customer Support. Improper use could result in system downtime or degraded performance.

Using the Storage Manager Parameters

The Storage Manager lists all components of the shared storage network in a tree view. You can view events for:

- All components in the shared storage network — Select all active Avid ISIS systems in the Selection window (the highest level in the tree view).
- Any subset of components — Select one or more entries in the Selection window (at a level lower than the Avid ISIS Systems in the tree view).



You must run the Storage Manager Parameters tool from a system with network access to the entire shared storage network. Otherwise, the tool cannot collect logs for all systems connected to the network.

To open the Storage Manager Parameters tool:

1. Do one of the following:

- ▶ (Windows) Select Start > Avid > Toolbox > Avid ISIS Toolbox.
- ▶ (Macintosh) Select Applications > AvidISISTools > ISIS Toolbox.

If any site security warnings open, click Yes to accept the certificate. If you are not sure about the security requirements of your shared storage network, see your system administrator.

The Avid ISIS Toolbox opens.

2. Click Storage Manager in the left pane.

The Storage Manager window opens.

To close the Storage Manager Parameters tool:

1. Click Close.

A dialog box opens asking you to confirm that you want to quit the ISIS Toolbox.

2. Click Yes.

Retrieve Storage Manager Flag Parameters

To use the Storage Manager Flag Parameters, you must have Administrative privileges and be logged into a system with access to the shared storage network.

To retrieve the Storage Manager Parameters:

1. Open the Storage Manager Parameters. (For information on opening the Storage Manager, see [“Using the Log Aggregator Tool” on page 125.](#))
2. In the Selection window, do one of the following:
 - ▶ Select all active Avid ISIS systems to view events from all components in the shared storage network.
 - ▶ Select one or more Storage Manager to view events from specific System Director.



3. Click Configure.

The Storage Manager Parameters dialog box opens.

4. Configure the following options to retrieve data:

Option	Description
No Filter	Selects all of the parameters listed in the Storage Manager Parameters window.
All other Storage Manager Parameters	Allows you to select one or multiple parameters listed in the Storage Manager Parameters window.
Log Level and Throttle	Do not change the Log Level or Throttle setting unless instructed to do so by Avid Customer Support. Improper use could result in system downtime or degraded performance.



5. Click OK to close the Storage Manager Parameters dialog box.

6. Click Start.

The Storage Manager displays the retrieved information.

Switch Manager Tool (ISIS | 7500)

The Avid ISIS Switch Manager tool allows you to retrieve and save error messages and/or reset the error count for any chassis switch (ISS or IXS).

To retrieve and save switch error messages:

1. Select Start > Avid > Avid ISIS Toolbox.

If any site security warnings open, click Yes to accept the certificate. If you are not sure about the security requirements of your shared storage network, see your system administrator.

The Avid ISIS Toolbox opens.

2. Click Switch Manager in the left pane.

The Switch Manager window opens.

3. In the Switches area, do one of the following:

- ▶ Select Avid ISIS Systems to retrieve error messages from all active switches in the media network.
- ▶ Select one or more switches to retrieve error messages from specific switches attached to the network.

4. Choose Retrieve Switch Errors from the Action list.



5. Click Start.

The Status area displays the results of the retrieve operation.



6. (Option) To save retrieved error messages, do the following.

- a. Click Save Results.

The Save Results dialog box opens.

- b. Choose a location on your system where you want to save the results.
- c. Type a file name into the File Name text field.
- d. Click Save.



The results are saved in Comma Separated Values (.csv) format by default.

To reset the switch error count:

1. Do one of the following:

- ▶ (Windows) Select Start > Avid > Toolbox > Avid ISIS Toolbox.
- ▶ (Macintosh) Select Applications > AvidISISTools > ISIS Toolbox.

If any site security warnings open, click Yes to accept the certificate. If you are not sure about the security requirements of your shared storage network, see your system administrator.

The Avid ISIS Toolbox opens.

2. Click Switch Manager in the left pane.

The Switch Manager window opens.

3. In the Switches area, do one of the following:

- ▶ Select Avid ISIS Systems to reset error counts from all active switches in the media network.
- ▶ Select one or more switches to reset error counts from specific switches attached to the network.

4. Choose Retrieve Switch Errors from the Action list.



5. Click Start.

The Status area displays the results of the reset operation.

To close the Switch Manager:

1. Click Close.

A dialog box opens asking you to confirm that you want to quit the Switch Manager.

2. Click Yes.

Network Utilities Page

The Network Utilities page provides you with the following standard utility tests:

- Network Statistics—displays statistics for IPv4 and IPv6, TCP and UDP
- Ping—allows you to test the connection between a system in the shared storage network and the System Director
- Traceroute—allows you to verify the path between a system in the shared storage network and the System Director



You must have Administrator privileges to run the utility tests.

To open the Network Utilities page:

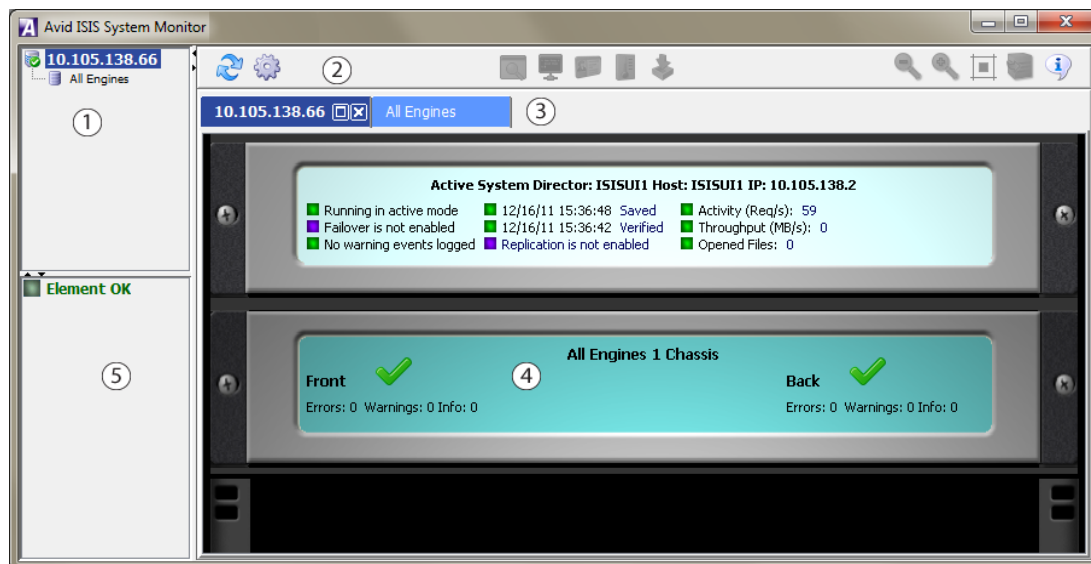
1. From the Management Console home page, click the Network Utilities icon, located in the Tools section.
The Network Utilities page opens.
2. Select Network Statistics, Ping, or Traceroute from the Command list.
3. Enter the network name or IP address of the target machine in the “Target name” field.
4. Click Submit to perform the command.

The results of the command are shown in the Results area.

Monitor Tool (ISIS | 7500)

The Monitor Tool provides detailed monitoring of all hardware components in the Avid ISIS media network on ISIS | 7500 systems only. The Monitor Tool displays overview information about the network hardware as a graphical representation of the current configuration, so you can view the components remotely to assess their functional status.

The Monitor Tool provides various views of the components in the media network and polls the System Director at timed intervals to update network data. On the left is the Navigation panel, which provides a tree view of the media network. On the right is the System panel, which presents system hardware components in a graphical display. You can view the network hardware at several levels: system, racks, chassis, or blades. At each level, the tool displays indicators of the health of the component, usually as a graphical representation of the actual LED state viewed on the component.



-
- | | |
|---|---|
| 1 | Navigation panel—Provides a tree view of media network components |
| 2 | Tool bar—Perform various actions depending on the view |
| 3 | Tab bar—Manage system monitor windows |
| 4 | System panel—Presents system hardware components in a graphical display |
| 5 | Legend panel—displays summary of all status messages |
-

The Monitor Tool also provides information about the physical location of each component. For example, the tool shows the chassis ID of each blade so that it can indicate the location of a malfunctioning blade within a chassis. The Monitor Tool does not track how racks or chassis are actually organized, but you can input site-specific data so that the tool can represent groupings of components in a way that makes sense in relation to how a specific media network is organized.

Accessing the Monitor Tool

To open the Monitor Tool:

1. Do one of the following:
 - ▶ (Windows) Select Start > Avid > Monitoring Tool> Avid ISIS Monitoring Tool.
 - ▶ (Macintosh) Select Applications > AvidISISTools > ISIS Monitoring Tool.



If the Monitoring tool is not installed, see “ISIS Toolbox” on page 123.

2. If any security warnings open, click Yes to accept the certificate. If you are not sure about the security requirements of your media network, see your system administrator.

The Avid ISIS System Monitor tool opens.

Configuring the Monitor Tool

By default the Monitor Tool shows all the Engines together in the same rack view regardless of physical configuration. You can customize the view by creating “virtual” racks in the Monitor Tool and populating them with Engines to reflect the layout of your physical rack system. You can then save your customizations for use during subsequent sessions.



To create a rack or add a rack to the Racks list:

1. From the Avid ISIS System Monitor window, click Configure.

The Rack Configuration dialog box opens.



2. Click Create.

The New Rack dialog box opens.

3. Type a rack name, and click OK.

The new rack is added to your configuration and displays in the Racks list in the left pane of the Rack Configuration dialog box.

4. (Option) Repeat this procedure to add additional racks.

To rename a rack:

1. Click to select the Rack you want to rename from the Racks list.



2. Click Rename.

The Rename Rack dialog box opens.

3. Type in the new Rack name and click OK.

The Rack name is changed.

To add one or more Engines to a rack:

1. Click to select the Rack to which you want to add Engines from the Racks list.



When you create a new rack, it is selected by default.

2. Click to select one or more Engines from the Unrackd Engines list on the right pane of the Rack Configuration dialog box.

You can select multiple Engines using Shift-click and Ctrl-click. See [“Selecting Items” on page 26](#) for more information on selecting multiple items.



3. Click Insert Engine.

The selected Engines are moved to the Racks list under the selected Rack.

To remove one or more Engines from a rack:

1. Click to select one or more Engines from the Racks list.

You can select multiple Engines using Shift-click and Ctrl-click. See [“Selecting Items” on page 26](#) for more information on selecting multiple items.

2. Click Remove.

The selected Engines are removed from the rack.

To remove a rack:

1. Click to select a Rack from the Racks list.

2. Click Remove.

The selected Rack is removed from the Racks list.

To save the configuration:

- Click Save Configuration.

To rearrange the placement of a chassis displayed in the Rack tab:

1. Click to select the chassis you want to move.

A yellow frame highlights the active chassis.

2. Drag and drop the chassis to a new location in the Avid ISIS System Monitor window. A red insertion line appears when the chassis is moved to an appropriate position.



Viewing Information in the Monitor Tool

Once you have configured the Monitor Tool for your media network, you can use the tool's graphical interface to view the status of your hardware components and retrieve information about its operation.

You can access the Avid ISIS Agents and view more information about Storage Managers and chassis switches by right-clicking the component in the Monitor Tool and selecting the appropriate IP address. For information on the Avid ISIS Agents, see [“Avid ISIS Storage Manager Agent” on page 141](#) and [“Understanding the Switch Agent Interface” on page 155](#).

To view information about the components of your media network:

1. Open the Monitor Tool (see [“Accessing the Monitor Tool” on page 133](#)).
2. Do one of the following to select the rack whose components you want to monitor:
 - ▶ In the Tree View pane, click the appropriate Rack element.
 - ▶ Click the appropriate Rack element in the graphical Rack pane.

The Monitor Tool displays a graphical representation of the rack element.



3. (Option) To view the other panel of the rack (either front or back), do one of the following:
 - ▶ Click Rotate Rack View to view the back panel of the rack.
 - ▶ Right-click a component, and select Rotate Rack View.

The Monitor Tool displays the other panel of the selected rack. You can use the Rotate Rack View to switch between back and front views.

4. Move the mouse pointer over a component to view information about its status and performance.

A tool tip window opens.

```
Avid ISIS Storage Element
Name: SM010
Version: 4.7.0.14335
Storage Blade Type: i2000
IP Address: 10.105.138.79
IP Address: 10.105.138.15
Slot number: 12
Status: Element OK
Temperature: 30°C
Network: OK
State: Active
Reported: 05/12/14 15:04:52
```

5. Use the following buttons to adjust your view of all components in the rack:

Symbol	Name	Description
	Zoom Out / Zoom In	Zooms in or out on the rack components view
	Reset View	Resets the zoom to the default for the window size
	Refresh	Updates the rack component view

Displaying Rack Configurations in Separate Windows

You can detach any rack tab so you can view it in a separate window. This allows you to keep a specific rack configuration visible while you configure other racks. You can also set the detached display to keep it on top of any active window on your desktop.

To detach a rack tab:



- ▶ Click Maximize button on the rack tab you want to display in a separate window.

To return a detached rack tab to the Avid ISIS System Monitor window:

- ▶ Close the detached rack tab window. The tab is restored to the Avid ISIS System Monitor window.

To close a rack tab:



- ▶ Click Close on the rack tab you want to close.

Understanding the Monitor Tool Views

The Monitor Tool allows you to select different views to see specific information about the network or about an individual component.

Using System View

General View displays each of the Storage Managers, chassis switches, and power supplies in your configuration. Managers flash gray if there is no communication between the System Director and a rack — for instance, if an Avid ISIS Storage Blade (ISB) is rebooting. Managers currently experiencing a failure appear grayed out. The Monitor Tool displays a Component Missing icon for any empty Storage Manager, chassis switch, or power supply slot that is empty.

In addition, the Monitor Tool displays the following symbols to indicate problems with the Storage Managers.

Symbol	Name	Description
	Upgrade	Indicates the element is currently undergoing a software upgrade. For more information on upgrade status, see “Using Upgrades View” on page 138 .
	Warning	Indicates the element has returned a warning message — for example, the Storage Manager might be rectifying or redistributing files.
	Error	Indicates the element has experienced a failure — for example, a disk failure.
	Info	Indicates one or more information messages are available for the element.

To see the System view:



- 1. Open the Monitor Tool (see “Accessing the Monitor Tool” on page 133).
- 2. Click System View.

Using Status Details View

In Status Details view, you can view comprehensive status details of each component in your configuration. Status indicators appear if status information is currently associated with a component. For a description of status indicators, see “Status Indicators” on page 137.

If no status information is associated with a component, the component appears green in Status Details view.



To see the Status Details view:

- Click Status Details View.

Status Indicators

The Status Details view displays the following status information. You can toggle between front and back views to see the status of Storage Managers, switches, and power supplies.



Not all status indicators are available for each component.

Status Details Information

Icon	Description (Storage Managers)	Description (switch)	Description (power supply)
	Connection error		
	Version mismatch	Version mismatch	
	Installing in progress	Installing in progress	

Status Details Information (Continued)

Icon	Description (Storage Managers)	Description (switch)	Description (power supply)
	Redistributing in progress		
	Rectifying files		
	Repairing mirrors		
	Disk failure	Stack error	
	Diagnostic mode		
	Network degraded	Trunking error	
	Disk degraded	Chassis error	
	Memory error		No power
	Redistribution information available		
	Manager offline		
		Link warning	

Using Blade Identification View

In Blade Identification view, you can view the names of each Storage Manager in your configuration.

**To see the Blade Identification view:**

- Click Blades ID View.

Using Temperatures View

In Temperatures view, you can view the temperature status of each Storage Manager in your configuration. Temperatures view lists the temperature of each Storage Manager, as well as a color-coded marker to indicate its status:

- Green (Normal): the temperature of the Storage Manager is under 60°C (140°F).
- Yellow (Warning): the temperature of the Storage Manager is between 60° – 70°C (140° – 158°F).
- Red (Critical): the temperature of the Storage Manager exceeds 70°C (158°F).

**To see Temperatures view:**

- Click Temperatures View.

Using Upgrades View

In Upgrades view, you can view the upgrade status of each element in your configuration. Upgrades view lists each Storage Manager with a color-coded marker to indicate whether or not it is being upgraded:

- Green: no upgrade is being installed.
- Blue: an upgrade is in progress.

- Orange: the upgrade installation failed.
- Yellow: the upgrade is waiting for components to complete installation before restarting

Upgrades view also highlights any mismatch between the version number of a component and the rest of the components in the chassis. If a component was not upgraded when the rest of the components in the chassis were upgraded, Upgrades view marks the component with a yellow Version Mismatch indicator with red text.



To see Upgrades view:

- ▶ Click Upgrades View.

Agent Settings Page

The Avid ISIS Management Console includes several tools for viewing the System Agent statistics and configuration information, and for configuring advanced options.



These tools should not be used unless under the advice and supervision of Avid support personnel.

- Use Agent Options to modify Agent configuration options.
- Use Agent Trace Setup to configure Agent trace settings for connections, HTTP requests, SSL callbacks, and threads.

Monitoring Avid ISIS with SNMP

You can use your Network Management System (NMS) or Simple Network Management Protocol (SNMP) management application to monitor ISIS-related system events on your Avid ISIS System Director.



Avid ISIS System Director supports unidirectional (read-only) SNMP communication only. Bidirectional communication is currently not supported.

A MIB (Management Information Base) file is available in the following location on the System Director:

D:\Program Files\Avid\ISIS System Director\ISIS.mib

You can import this MIB into your NMS so that you can monitor and manage Avid ISIS events. For more information, see your NMS documentation. For a more detailed overview of the Avid ISIS MIB, see [“Avid ISIS SNMP MIB Reference” on page 171](#).

The following System Director events can be monitored with SNMP:

Category	Name	Description
Product		
	ISIS_ProductName	Shows the name of the ISIS product line
	ISIS_Version	Shows the version of the ISIS install
Status		

Category	Name	Description (Continued)
	ISIS_SystemDirectorState	Shows the state of the System Director: • 0=Online • 1=Offline • 2=Standby • 3=Unknown
	ISIS_SystemDirectorStateString	Shows the state of the System Director in string format
	ISIS_CheckEventLog	Shows whether the check event log flag is set
	ISIS_WorkspaceRedistributingCount	Shows the current number of workspaces currently performing a redistribution
Performance		
	ISIS_MegabytesPerSecond	Shows total megabytes per second for all connected clients
	ISIS_ReadMegabytesPerSecond	Shows total read megabytes per second for all connected clients
	ISIS_WriteMegabytesPerSecond	Shows total write megabytes per second for all connected clients
	ISIS_MessagesPerSecond	Shows the number of messages per second the System Director is processing
	ISIS_OpenFiles	Shows how many files are currently open
	ISIS_ActiveClientCount	Shows the active client count
	ISIS_MaximumClientCount	Shows the maximum active client count
Usage		
	ISIS_HighestDiskUsedPercentage	Shows the highest percent used across all disks
	ISIS_TotalSystemMB	Shows the total system megabytes
	ISIS_TotalAllocatedMB	Shows the total allocated megabytes. Allocated size is the sum of all the workspace sizes.
	ISIS_TotalUsedMB	Shows the total system usage across all workspaces
	ISIS_FileCount	Shows the total number of files across all workspaces
	ISIS_FolderCount	Shows the number of folders across all workspaces
	ISIS_WorkspaceCount	Shows the total number of workspaces

A Avid ISIS Storage Manager Agent

You can view detailed information about all Storage Managers connected to the shared storage network by using Avid ISIS Agents. The Agents run as a Web service on the Storage Managers, and can be accessed during normal system operations from the ISIS Management Console.



You must have Administrator privileges to access the Agents.

Opening the Avid ISIS Storage Manager Agent

The Avid ISIS Storage Manager Agent runs within a web browser window. You can open the Agent pages from either the Management Console or the ISIS Launch Pad.

The following are the default Agent passwords. For more information about changing the Agent Administrator password, see [“Changing the Agent Administrator Password \(ISIS | 5500 and 2000 only\)” on page 149](#).

- ISIS | 5500 Agent page password is: — is-admin
- ISIS | 7500 and ISIS | 2500 Agent page password is: — se-admin



On any ISIS system, you can also use the ISIS Administrator password to access the Agent pages.

To open the Storage Manager Agent:

1. Do one of the following:

- ▶ From the Storage Managers tool, select an IP address from the IP Addresses panel of the Details panel, and click Info. For more information, see [“Viewing Storage Manager Details” on page 35](#).
- ▶ From the System Director desktop, click the “Launches the Agent Management Page” button on the ISIS Launch Pad.” For more information, see [“ISIS Launch Pad” on page 49](#).

The Storage Manager Agent page opens.

2. Type the Administrator password into the password field and do one of the following:



- ▶ Click the arrow icon.
- ▶ Press Enter.

The Agent page opens.

Effect of Changing the Agent SSL Setting

For the Admin Server Agent, by default, SSL is enabled on the ISIS | 7500, and disabled on ISIS | 5500 and ISIS | 2500. (SSL is enabled on all ISIS models for the Storage Manager Agent.)

The following tables describe the required login access when SSL is set to the default or not. Changing the default setting is not common and should be done only with the guidance of Avid support. For information on changing the SSL setting, see [“Agent Settings Page” on page 139](#).

In each case, you can use either the IP address or the host name (if applicable) of the server.

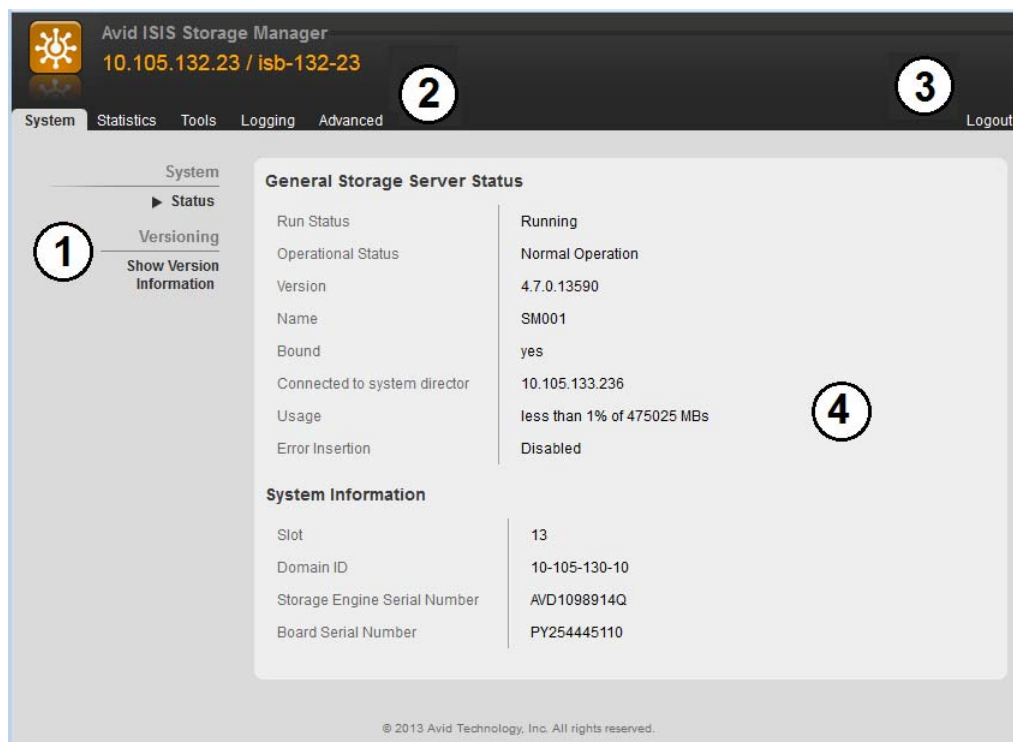
ISIS Model	SSL Setting	Admin Server Agent Login
7500	ON (default)	https://IP-addr:5015
	OFF	http://IP-addr:5015
5500	OFF (default)	http://IP-addr
	ON	https://IP-addr
2500	OFF (default)	http://IP-addr
	ON	https://IP-addr

ISIS Model	SSL Setting	Storage Manager Agent Login
All	ON (default)	https://IP-addr:5015
	OFF	http://IP-addr:5015

Understanding the Agent Interface

The Avid ISIS Agent, which you can run on the System Director or any Ethernet-attached client, has a user interface where controls are grouped by function and are displayed by clicking the appropriate buttons.

The following figure illustrates the Avid ISIS Storage Manager Agent with the System tab selected. Depending on your ISIS model, the options in each tab can vary.



The Agent is divided into the following areas:

1	Command menu—Contains the options used for basic management functions.
2	Tabs—You can access different Command functions by clicking the tabs at the top of the Agent tool. The System tab is selected by default.
3	Logout link
4	Main display area—Displays information about your network and allows you to configure components.

System Tab

The System tab allows you to view configuration information for Storage Managers. The System tab lists general information about component status, version, and usage. On an ISIS | 5500, you can also change the Management Console Administrator password and manage Storage Manager Agent profiles.

Menu	Heading	ISIS Model	Displayed Information
System	Status	All	General Storage Server Status: - Run Status - Operational Status - Version - Name - Bound - Connected to System Director - Usage - Error Insertion
System (continued)	Status	All	System Information: - Storage Engine Serial Number (All) - Engine Controller Slot (2500) - Engine Controller Serial Number (2500) - Storage Engine Part Number (2500) - Engine Controller Part Number (2500) - Storage Engine ID (2500) - Slot (7500) - Domain ID (7500) - Board Serial Number (7500 and 5500) - Chassis Serial Number (7500 and 5500)

Menu	Heading	ISIS Model	Displayed Information
Configuration	Status	5500 and 2500	Hardware Status: - Status - Product Part Number - BMC - System Temp (2 on the 5500; 14 on the 2500) - Fan (5 on the 5500; 3 on the 2500) - Power Supply (2 on each)
		5500	- CPU Temp (2) - System Drive
	System	5500	Naming - Host Name - Nameservers Administrative Password You can change the Storage Manager Agent Administrator password; for more information, see “Changing the Agent Administrator Password (ISIS 5500 and 2000 only)” on page 149
	Network	2500	You can configure the network information in this area, including the hostname, default gateway, data interfaces, and management interfaces. For more information, see the <i>Avid ISIS 2500 Setup Guide</i> .
	Time	2500	You can configure up to two network time servers in this area, or enter the date and time manually. For more information, see the <i>Avid ISIS 2500 Setup Guide</i> .
Profile	Administration	2500	You can change the Storage Manager Agent Administrator password in this area; for more information, see “Changing the Agent Administrator Password (ISIS 5500 and 2000 only)” on page 149  Never use the Command Line to change the Administrator’s password, doing so would prevent all future log-ins.
	View all	5500	Displays the version running on the ISIS (System Build Information) and any Agent profiles that have been created
	Create new	5500	Clicking this link creates a new Agent profile, displays it on screen, and adds the profile to the profiles list; for more information, see “Creating New Storage Manager Agent Profiles” on page 148
	Delete this	5500	Clicking this link deletes the currently displayed Agent profile; for more information, see “Deleting Agent Profiles” on page 149  <i>This link appears only when an Agent profile is being displayed</i>
	Delete all	5500	Clicking this link deletes all Agent profiles; for more information, see “Deleting Agent Profiles” on page 149
Versioning	Show Version Information	7500 2500	Displays current software version of the Storage Manager.

Statistics Tab

The Statistics tab displays basic information about your network or network components and provides statistics for the local system and for the Storage Manager.

Menu	Heading	ISIS Infrastructure	Description
Local System	General	7500 5500	System Information: • Computer Name • OS Version • Processor Type • Number of Processors • System Uptime • Serial number (7500, 2500) Memory Information: • Total Physical Memory • Total Physical Memory Usage • Available Physical Memory • Total Page File • Available Page File
	Agent	All	• Agent Environment • Agent Statistics • Agent Configuration • Browser Details
Storage Manager	General	All 7500	• Storage Manager General Statistics • Parity RAID Specific Statistics
	Disk	All	Displays detailed information about disk or array properties and disk use
	Disk S.M.A.R.T.	7500	Retrieves S.M.A.R.T. statistics for the Storage Manager S.M.A.R.T. is an industry-standard reporting method.
	Redistribution	All	Displays information about the Storage Manager's status during current redistribution pass, and lists Storage Managers that are having problems with the current redistribution pass
	Performance	All	Displays information about the Storage Manager's performance
	Network	All	Displays information about the current network status and connectivity between the Storage Manager and the System Director

Tools Tab

The Tools tab provides you with network tools and component utilities that generate basic information on network functioning and low-level information on Storage Managers and switches. These tools are used primarily by Avid Customer Support to diagnose problems with components of the shared storage network.

The Tools tab for Storage Managers provides access to the Console Viewer. For information on the Console Viewer, see [“Using the Log Viewer Tool” on page 153](#).

Tool	Heading	ISIS Infrastructure	Description
General Tools	• ping	All	Allow you to test the connections between components in the shared storage network, to verify the path between components, and to run the Linux df command
	• traceroute		
	• df (disk free) or Disk Space Usage		
Blade Tools	• istate	7500 — all	Allow you to run low-level tests to generate data to identify problems with components in the shared storage network
	• ivers	headings	
	• i2cio	2500 — istate and ivers headings	
	• route show		

Logging Tab

The Logging tab provides a complete view of the logs of active Storage Managers. The logs provide you with a system snapshot of error and status messages. The logs provide detailed status information that is especially useful to Avid Customer Support personnel for monitoring system status during prolonged operations.

Tool	Heading	ISIS Infrastructure	Description
System	Entries to view	All	Specifies the number of entries to view. Specify 0 to view all entries
	Log to view	All	Selects the log to view: On 7500 and 2500, select a message log by its suffix number
	Log to clear	All	Selects the log to clear: On 7500 and 2500, select a message log by its suffix number
	Kernel Ring Buffer	7500 2500	The Kernel Ring Buffer displays logs maintained by the Linux kernel. These logs are used by Avid Customer Support
Storage Manager	Disable/Enable logging	All	Enables and disables the logging function for the individual Storage Manager
	Dump current log	All	Saves the current log to a file and makes it available for download

Tool	Heading	ISIS Infrastructure	Description (Continued)
	Log filter	All	This option appears only when you disable logging. Select the logs you want to capture. Select No filtering if you want all the logs.
	View available logs	All	Displays the logs that have been previously saved
	Delete all logs	All	Deletes all log files on the current Storage Manager
	Dump all peer logs	All	Saves the logs of all Storage Managers in the current chassis to files
Storage Engine	Dump engine log	2500	Saves the current Engine log to a file and makes it available for download

Advanced Tab

The Advanced tab contains configuration utilities, installation logs, and diagnostic tools used by Avid Customer Support personnel used to troubleshoot problems with the shared storage network. You can also use the Advanced tab in the ISIS | 7500 to set the integrated switches back to the factory defaults. This might be necessary to reset the IP addresses of system components if your Avid ISIS system experiences network communication problems.



Use of the tools in the Advanced tab can result in degraded system performance or loss of data. The tools should be used by Avid Customer Support personnel or under Avid Customer Support direction.

Tool	Heading	ISIS Infrastructure	Description
System Tools	Reboot	7500 2500	Restarts the system. This function requires the Administrator password.
	ShutDown	2500	Sends a shutdown command the ISIS 2500 Engine. This function requires the Administrator password. Allow 1 minute for the buffers to clear, then you can turn off the power to the Engine. Once this command has been sent, the Engine needs to be power cycled before the Engine can turn back on (turn both Engine power switches off and on).
	Issue Shell Command	7500 2500	Provides a text field to issue shell commands. Only Avid support personnel should use this functionality.
Agent Settings	Configuration	All	Add or change configuration option values.
	Management Port Configuration	2500-2000	Configure a Management Port on one of the Storage Managers.
Installation Logs	*.log	7500 2500	Provides read-only access to Storage Manager installation logs.
Storage Manager	Unbind	All	Unbind a bound Storage Manager. This function requires the Administrator password.
	Error Insertion	All	Simulate various errors to diagnose a Storage Manager.

Tool	Heading	ISIS Infrastructure	Description (Continued)
	Redistribution Near Full Threshold	All	Displays the remaining free block count before the ISBs start prioritizing moving blocks off of it over accepting new data so that it doesn't get filled up and wedged before it has enough time to delete older blocks. This typically happens during full redistributions when the system is greater than ~80% full. The default of 2000 blocks is typically good for most situations. This option gives Avid Customer Support the ability to change the field when needed. This function requires the Administrator password.
Disk Tools	Log Physical Configuration	5500 2500	Logs the current configuration of the disks
	Clear Foreign Configuration	5500 2500	Clears the configuration on the disks and permanently deletes all data from those disks. This function requires the Administrator password.
RAID Diagnostics	Verify RAID Configuration	2500	Verifies the current configuration of the RAID set (number of arrays and spares)
	Show RAID Configuration	2500	Displays the current configuration of the RAID set (number of arrays and spares) with details of each disk and slot
	Show RAID Status	2500	Displays details about the low level RAID status
	Create RAID Configuration	2500	Creates a RAID set. If a RAID set already exists, the operation fails.
RAID Tools	Storage Manager Rescan	5500 2500	Refreshes the status of the RAID set in the Engine to the System Director. The Status in the agent page System tab is one of many places that is updated.
	Repair Configuration	2500	Attempts to do a non-destructive repair of the RAID configuration (not to be confused with a drive repair/rebuild).
Destructive RAID Tools	Delete and Recreate	2500	Recreates the RAID configuration on the disks and permanently deletes all data from those disks. This function requires the Administrator password.

Managing Storage Manager Agent Profiles (ISIS | 5500)

Storage Manager Agent profiles contain information about the current versions of required software, drivers, and hardware components that are installed on a Storage Server. You can view, save, or delete profiles, but you cannot use the Profile tool to edit or modify the information.

Profiles are typically used by Avid Customer Support to help determine problems with installed versions of the operating system, drivers, adapter boards, or firmware.

Creating New Storage Manager Agent Profiles

To create a new Storage Manager profile:

- From the Manager Agent System tab, click “Create new” in the Profile section.
A new Manager Agent profile is created and displayed on screen.



The profile is automatically saved, and can be viewed at a later time using the [View all](#) link. For more information, see [“Viewing Storage Manager Agent Profiles”](#) on page 149.

Viewing Storage Manager Agent Profiles

Once you have created at least one profile, you can use the “View all” link to retrieve them at any time.

To view profiles:

1. From the Manager Agent System tab, click “View all” in the Profile section.
The profile viewer page opens.
2. Click Open for the profile that you want to view.
The selected profile opens.

Deleting Agent Profiles

You can delete the currently displayed profile, any, or all saved profiles.

To delete the currently displayed profile:

1. Click “Delete this” from the left side menu.
A confirmation dialog opens.
2. Click Yes.
The currently displayed profile is deleted, and the “View all” page opens.

To delete any profile:

1. From the “View all” page, click Delete for the profile you want to delete.
A confirmation dialog opens.
2. Click Yes.
The selected profile is deleted.

To delete all profiles:

1. Click “Delete all” from the left menu.
A confirmation dialog opens.
2. Click OK.
All profiles are deleted.

Changing the Agent Administrator Password (ISIS | 5500 and 2000 only)

By default the Agent Administrator password is set to “is-admin.” or “se-admin.” Change this password the first time you use the Agent page.



Never use the Command Line to change the Administrator’s password; doing so prevents all future log-ins.

To change the Agent Administrator password:

1. Click System, under Configuration in the System tab.
2. In the Administrative Password section, do the following:
 - a. Type the current password in the “Current Password” field.
 - b. Type the new password in the “New Password” field.
 - c. Type the new password again in the “Confirm Password” field.
 - d. Click Submit.

The Agent Administrator password is changed to the new value.

Storage Manager Logging

The Logging tab provides a complete view of the logs of active Storage Managers. The logs provide you with a system snapshot that you can use to view error and status messages. The logs provide detailed status information that is especially useful to Avid Customer Support personnel for monitoring system status during prolonged operations.

Using Storage Manager Agent Logging

You can use the Logging tab to view event logs and to clear existing logs. The Logging tab contains two main sections:

- Options section—The left section allows you to select specific logging options to display and to perform administrative tasks relating to the Agent logs.
- Logs section—The right section displays different types of events and information from the network components.

To access Agent Logging functions:

1. Open the Agent. (For information on opening the Agent, see [“Opening the Avid ISIS Storage Manager Agent” on page 141.](#))
2. Click the Logging tab.

The Logging window opens.

Viewing Agent Event Logs

To view event logs:

1. Open the Agent. (For information on opening the Agent, see [“Opening the Avid ISIS Storage Manager Agent” on page 141.](#))
2. Click the Logging tab.
The Logging window opens.
3. In the Entries to view text box, type the number of events to display. The default is 100. If you want to view all events, type “0” (zero) in the Entries to view text box.
4. Select a log from the “Log to view” list.
5. Click View.

The event log displays in the Logs area.

Clearing Agent Event Logs

You can clear the logs in any of the logging categories. This empties the log of all event entries and resets the logging process.

To clear logs:

1. Open the Agent. (For information on opening the Agent, see [“Opening the Avid ISIS Storage Manager Agent” on page 141.](#))
2. Click the Logging tab.
The Logging window opens.
3. Select a log from the “Log to clear” list.
4. Click Clear.
5. Click OK.

The event log is cleared, and logging is reset to start recording new events.

Resetting the Storage Manager Status (ISIS | 2500)

A single Engine Controller in an ISIS | 2500-240 Engine controls two Storage Managers. Use the instructions in this section if the two Storage Managers are reporting the following status:

- Hot spare drive is missing
- Foreign disk
- Invalid spare drive slot

Correcting the Storage Managers status is a two step process. Perform one procedure on one of the Storage Managers and the second procedure on the second Storage Manager.

On one of the Agent pages:

1. Open the Storage Manager Agent. (For information on opening the Agent, see [“Opening the Avid ISIS Storage Manager Agent” on page 141.](#))
2. Click the Advance tab.
The Advance window opens.
3. Select “Clear Foreign Config” from the “Disk Tools” list.
4. Type the administrator password in the Password text box (default is se-admin) and click Clear.

On the second Agent page:

1. Open the Storage Manager Agent. (For information on opening the Agent, see [“Opening the Avid ISIS Storage Manager Agent” on page 141.](#))
2. Click the Advance tab.
The Advance window opens.
3. Select “Storage Mgr Rescan” from the “RAID Tools” list.
The result of the Storage Manager rescan is displayed.
The Storage Manager status configuration is now corrected.

Enabling and Disabling Storage Manager Logging

Do not disable logging on a Storage Manager unless instructed by Avid support. Disabling logging for a Storage Manager does not affect system logging functions.

To stop the logging function:

- ▶ Select “Disable logging” from the Storage Manager area.
 - A confirmation message appears in the logging window.
 - The “Disable logging” link changes to “Enable logging.”

To start the logging function:

- ▶ Select “Enable logging” from the Storage Manager area.
 - A confirmation message appears in the logging window.
 - The “Enable logging” link changes to “Disable logging.”

Saving Logs

To save the log displayed in the Logs area, do one of the following:

- ▶ Select “Dump current log” from the Storage Manager area.
- ▶ Select “Dump all peer logs” from the Storage Manager area.

The current log or all peer logs are saved, and the Logging window displays a list of saved logs.

Viewing and Deleting Saved Logs

To view a saved log:

1. Select “View available logs” from the Storage Manager area.

The Logs area displays a list of all available logs.

2. Locate the log you want to view, and click Download.

The Agent tool downloads the log to the specified directory on your local system.



Depending on your browser configuration, the log file might display in the browser window automatically.

3. Open the log file in a text editor.

To delete a saved log:

1. Select Storage Manager > View available logs.

The Logs area displays a list of all available logs.

2. Locate the log you want to delete, and click Delete.

A confirmation dialog box appears.

3. Click OK.

The log is deleted from the Agent system.

Using the Log Viewer Tool

The Log Viewer tool is a utility that displays event information about Storage Managers. You cannot save the information displayed in the Log Viewer tool, but you can copy it to a word processing application, such as Notepad. You can also save event logs displayed in the Logging tab (see “Saving Logs” on page 152). The information is used primarily by Avid Customer Support personnel to help analyze problems with Storage Managers.

To install the Log Viewer tool:

1. In the Management Console, click Installers under the System heading.
2. In the ISISTools section, click the Toolbox executable file appropriate for your operating system.
3. Save the executable file to your computer and install it.

To monitor event information about Storage Managers:

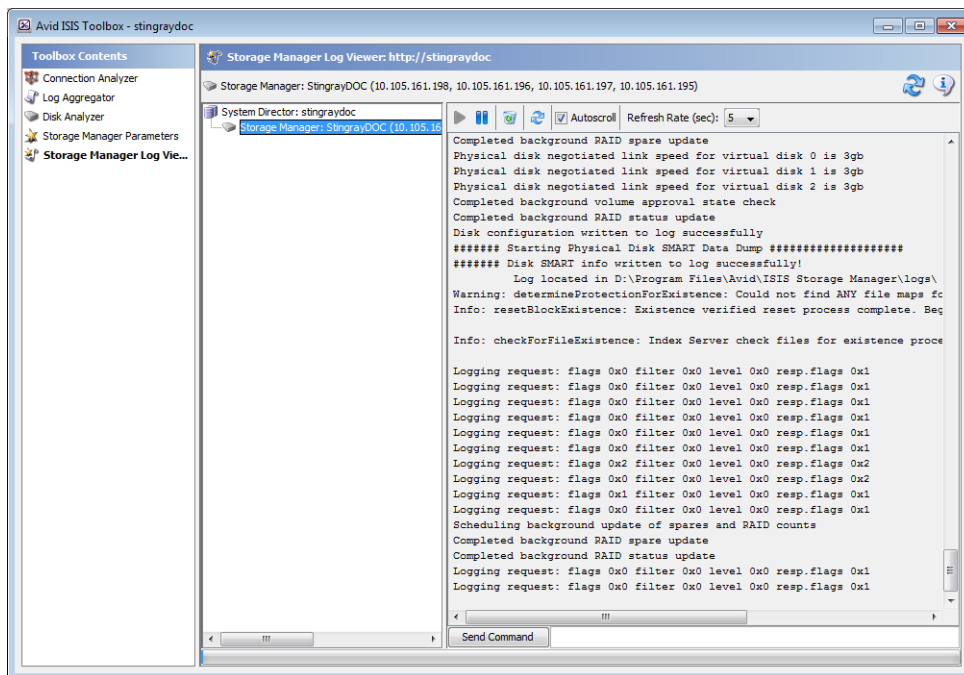
1. Do one of the following:
 - ▶ (Windows) Select Start > Avid > Toolbox > Avid ISIS Toolbox.
 - ▶ (Macintosh) Select Applications > AvidISISTools > ISIS Toolbox.

If any site security warnings open, click Yes to accept the certificate. If you are not sure about the security requirements of your shared storage network, see your system administrator.

The Avid ISIS Toolbox opens.

2. Click Storage Manager Log Viewer in the left pane.

The Log Viewer tool opens.



3. Select an option as described in the following table.

Option	Description
Resume	Resumes monitoring Storage Manager events

Option	Description (Continued)
Pause	Stops monitoring Storage Manager events
Clear	Clears all event data from the Console View tool
Resync	Restores previously-cleared event data to the Console View tool
Autoscroll	Scrolls the display to the bottom of the page
Refresh Rate (sec)	Sets the rate at which the Console View tool refreshes event data

B Avid ISIS | 7500 Switch Blade Agent

You can view detailed information about all ISIS | 7500 chassis switches connected to the media network by using the Avid ISIS Switch Blade Agents. The Agents run as a Web service on the chassis switches — Integrated Switch Blades (ISS) and ISIS Expansion Switch Blades (IXS). You can access the Agents during installation and configuration procedures by attaching a laptop to the Management port on the ISS or IXS, or you can access them during normal system operations from the ISIS Management Console.

You can also access the Agents from the System Monitor tool. For more information, see [“Hardware Monitoring Service” on page 115](#).



You must have Administrator privileges to access the Agents.

Understanding the Switch Agent Interface

The Avid ISIS Agent, which you can run on the System Director or any Ethernet-attached client, has a user interface where controls are grouped by function and are displayed by clicking the appropriate buttons.

The following figure illustrates the Avid ISIS Switch Blade Agent with the System tab selected.

Management Domain

ID	Revision	Request ID	Request Busy	Request Failures
10-105-130-10	1.02	2372	No	No

ID	Serial Number	FRU Health	Last Update	Side	State	Alerts	Type	CM	Stacking	Link Agg. / HG	Request State / ID
0	A/D1098914Q	OK	1s	Left	OK	None	ISS-2 (M)	2.44	Off	Acpt / Off	Done / 2372
1	DefaultSerial#	OK	25s	Left	OK	None	IXS-2 (B)	2.44	Up	Ready / Off	Done / 2372
				Right	OK	None	IXS-2 (M)	2.44	Up	Ready / Off	Done / 2372
2	A/D1084456C	OK	0s	Left	OK	None	ISS-2 (M)	2.44	Up	Ready / Off	Done / 2372
				Right	OK	None	ISS-2 (B)	2.44	Off	Acpt / Off	Done / 2372
3	PY258443001	OK	1s	Left	OK	None	ISS-2 (M)	2.44	Up	Ready / Off	Done / 2372
				Right	OK	None	ISS-2 (B)	2.44	Off	Acpt / Off	Done / 2372
5	A/D1098914V (Local)	OK	0s	Left	OK	None	ISS-2 (M)	2.44	Up	Ready / Off	Done / 2372
				Right	OK	None	ISS-2 (B)	2.44	Off	Acpt / Off	Done / 2372

Stacking Status

Switch Slot	State	Master	Collisions	Failures	10 Gb Port Map	Hi Gb Port Map
0	Ready	No	None	None	0x0	0x0
1	Ready	No	None	None	0x0	0x0

Stacking Database

```

Stack task current DB (5 Entries):
Entry 1/5: MAC: 00:a0:7e:0c:1e:76
Entry 2/5: MAC: 00:a0:7e:0c:32:ba
Entry 3/5: MAC: 00:a0:7e:0c:47:64 (MASTER)
Entry 4/5: MAC: 00:a0:7e:0c:48:f4
Entry 5/5: MAC: 00:a0:7e:0c:49:92 (local)
Discovery Timeout: 30000000 us
Topology Timeout: 10000000 us
Attach Timeout: 45000000 us
Discovery      Cos: 2  Vlan: 1
ATP           Cos: 2  Vlan: 1
Next Hop      Cos: 2  Vlan: 1
  
```

Stacking Port Status

```

Stacking_Port(56502:*hg0)      State: SW_PORT_STACKED
  
```

The Agent is divided into the following areas:.

- 1 Command menu—Contains the options used for basic management functions.
- 2 Tabs—You can access different Command functions by clicking the tabs at the top of the Agent tool. The System tab is selected by default.
- 3 Logout link
- 4 Main display area—Displays information about your network and allows you to configure components.

When you access Switch Blade Agents and submit a request for an action — for example, when you change the level of detail for chassis logs — a message tells you that the request was successfully or unsuccessfully submitted, and the progress of the request is reported to the Main display area.

Request Details for request id: 9065

Chassis Id	Chassis Serial Number	Switch Slot	Current Request Id	Current Request State	Current Request Errors
0	AVD1098914Q	0	2372	Done	Yes
		1	9065	Done	Yes
1	DefaultSerial#	0	9065	Done	None
		1	9065	Done	Yes
2	AVD1084456C	0	9065	Done	Yes
		1	9065	Done	None
3	PY258443001	0	9065	Done	None
		1	9065	Done	None
5	AVD1098914V	0	9065	Done	Yes
		1	9065	Done	None

System Tab

The System tab allows you to view configuration information for chassis switches. The System tab lists general information about component status, version, and usage. You can use the System tab to access information on any chassis switch (see [“Viewing System Information for Individual Chassis Switches” on page 161](#)). You can also add or remove chassis. For information on adding and removing network components, see the *Avid ISIS 7500 Setup Guide*.

You can also create, modify, and delete link aggregation configurations. Link aggregation, sometimes called trunking, allows you to combine physical network links into a single logical link for increased bandwidth. Link aggregation can increase the capacity and availability of the communication channel between devices (both switches and clients) using existing Ethernet technologies by combining two or more Ethernet connections to increase the bandwidth capability and to create resilient and redundant links. Link aggregation also provides load balancing where the processing and communications activity is distributed across several links so that no single link is overwhelmed.



Link aggregation is configured during setup and installation of your Avid ISIS media network. Changing the configuration can disrupt all link aggregation for your network and degrade system performance. Do not modify configuration values unless instructed to do so by Avid Customer Support.

Configuration values are set during installation and are displayed in the System tab. By default, the System tab displays general status information about the Storage Manager.

Menu	Option	Description
System	Overview	Displays a snapshot view of the status of switches and information about the stacking state and Management Domain ID number of the network chassis.
Configuration	Basic	Displays basic setup and configuration information about a chassis switch. Changing configuration IP addresses can affect network connectivity. The Basic option also allows you to set the date and time on a chassis switch. This resets the date and time for all Storage Managers in the chassis as well. For more information, see “Setting Chassis Time” on page 161 .
	Set stack password	Allows you to change the password for a chassis stack (maximum of 8 characters). Changing the stack password affects all connected Storage Managers and chassis in the stack.
	Reset Local Chassis ID	Allows you to change the ID number of the engine. Type the new ID number in the text box and click Submit. To clear the number you typed in the text box click Reset.
	Add/Remove chassis	Allows you to add a chassis to or remove a chassis from the network. For more information on adding and removing chassis, see the <i>Avid ISIS / 7500 Setup Guide</i> .
	Reboot a chassis	Allows you to reboot all Storage Managers and switches in a chassis at one time.
	Flush chassis manager logs	Allows you to dump all current chassis logs to the \var\log directory on the Storage Managers.
10 Gb Link Aggregation	View current settings	Displays the current configuration used for link aggregation, including the link type and the chassis port map
	Create new group	Allows you to define a new link aggregation group. Link aggregation is configured during setup and installation of your Avid ISIS 7500 media network. Changing the configuration can disrupt all link aggregation for your network and degrade system performance. Do not modify configuration values unless instructed to do so by Avid Customer Support.
	Enable/Disable	Lists the network link aggregation configurations for the chassis and allows you to enable or disable them. Enabling or disabling link aggregation affects all configurations in the network.
	Restart	Lists the network link aggregation configurations for the chassis and allows you to restart them. Restarting link aggregation stops all configurations in the network and restarts them.
	Delete configuration	Allows you to delete all of the current link aggregation configurations for your network.

Menu	Option	Description (Continued)
	Configure failover policy	Allows you to enable or disable failover for all current link aggregation configurations for your network. “Enable automatic failover for all networks” is set by default. Examples of the settings are as follows. - Failover enabled — For example, if three Link Aggregation ports are configured, traffic is evenly distributed over the three ports. If one of the links fail, the two remaining ports split the traffic. The overall bandwidth of the Link Aggregation group is less because only two of the three ports are working. The Link Aggregation group still works correctly. - Failover disabled — For example, if three Link Aggregation ports are configured, traffic is evenly distributed over the three ports. If one of the links fail, all traffic is stopped even though there are still have two working ports. The Link Aggregation group is marked as failed and no traffic is allowed.
Versioning	Show Version Information	Displays current software version of the component.

Statistics Tab

You can use the Statistics tab to view basic information about your network or network components. The Statistics tab provides you with statistics for the local system and for the switch.

Type	Description	
Local System	- General - Network - Agent	Displays detailed information about the chassis, including its components, the status of each part of the switch, and stacking information
Port Status	- View by chip - View by function	Displays information about port status grouped either by chip (matching the physical location of the port on the switch) or by function (for example, stacking ports or external client ports)
Port Errors	- View by chip - View by function - Reset all error counts	Lists port errors grouped either by chip (matching the physical location of the port on the switch) or by function (for example, stacking ports or external client ports); also allows you to clear all error counts

Tools Tab

The Tools tab provides you with network tools and component utilities that generate basic information on network functioning and low-level information on switches. These tools are used primarily by Avid Customer Support to diagnose problems with components of the media network.

Tool	Description	
General Tools	- ping - tracert - df (disk free)	Allow you to test the connections between components in the media network, to verify the path between components, and to run the Linux df command

Tool	Description (Continued)	
Blade Tools	• istate	Allow you to run low-level tests to generate data to identify problems with components in the media network
	• ivers	
	• i2cio	
	• route show	

Logging Tab

The Logging tab provides a complete view of the logs of active switches. The logs provide you with a system snapshot that you can use to view error and status messages. The logs provide detailed status information that is especially useful to Avid Customer Support personnel for monitoring system status during prolonged operations.

Tool	Description	
System	Entries to view	Specifies the number of entries to view. Specify 0 to view all entries.
	Log to view	Selects the log to view.
	Log to clear	Selects the log to clear.
	Kernel Ring Buffer	The Kernel Ring Buffer displays logs maintained by the Linux kernel. These logs are used by Avid Customer Support.

Advanced Tab

The Advanced tab contains configuration utilities, installation logs, and diagnostic tools used by Avid Customer Support personnel used to troubleshoot problems with the media network. You can also use the Advanced tab to set the integrated switches back to the factory defaults. This might be necessary to reset the IP addresses of system components if your Avid ISIS system experiences network communication problems.



Use of the tools in the Advanced tab can result in degraded system performance or loss of data. The tools should be used by Avid Customer Support personnel or under Avid Customer Support direction.

Tool	Description	
System Tools	Reboot	Reboots the switch.
	Issue shell command	Provides a text field to issue shell commands directly to the switch.
Agent Settings	Configuration	Adds or changes switch configuration option values.
System Files	bus_watcher	
Installation Logs	(*.log)	Provides read-only access to switch installation logs.
Switch Blade	Reboot an ISB	Restarts the selected Storage Manager (ISB).
	Reset to factory defaults	Resets the chassis to factory default settings; for more information, see “Resetting an Avid ISIS Engine to Factory Defaults” on page 162.
	Management port configuration	Changes the network settings for the Switch Blade management port.

Tool	Description (Continued)
Access configuration	Sets normal (default) or remote access to the switch.
Local Driver Diagnostics	Runs local switch driver diagnostic tests and display the results.
Switch Infrastructure Diagnostics	Runs system level diagnostic tests; for more information, see “Switch Infrastructure Diagnostics” on page 163 .
Restart Chassis Manager	Restarts the chassis manager software.
Set chassis manager log level	Allows you to set the level of detail collected in chassis logs: • Off • Normal (default) • Verbose The Chassis Manager — the application running on the switch — maintains logs and periodically collects them in a compressed file.
ISB heartbeat timeout	Automatically reboots the ISB if the switch does not get status from an ISB within a certain time limit. The check box is selected (enabled) by default.

Viewing System Information for Individual Chassis Switches

When you log in to a selected ISS or IXS, you can use the System tab of the Switch Blade Agent to access information about any switch, not just the selected one.

To view system information for a chassis switch:

1. Open the Switch Blade Agent (see [“Avid ISIS | 7500 Switch Blade Agent” on page 155](#)).
2. Click the System tab if it is not already selected.

The System window opens.

3. In the Management Domain area, click a switch listed in the Serial Number column.

The Agent displays information for the switch in the Main display area.

Setting Chassis Time

You can set the time for all Storage Managers connected to your chassis switch by using the Switch Blade Agent. You can also use a Network Time Protocol (NTP) server to establish the time for your system. Setting chassis time synchronizes the time for all Storage Managers and, in systems with multiple chassis, on all switches.



Only make changes to the settings listed in this procedure. Do not make changes to any other settings unless instructed to do so by qualified Avid support personnel.

To set the time for a chassis:

1. Open the Switch Blade Agent (see [“Avid ISIS | 7500 Switch Blade Agent” on page 155](#)).
2. Click the System tab if it is not already selected.

The System window opens.

3. Click Basic in the Configuration area.

The Chassis Configuration dialog box opens.

Configuration

- Basic
 - Set stack password
 - Reset Local Chassis ID
 - Add/Remove chassis
 - Reboot a chassis
 - Flush chassis manager logs
- 10 Gb Link Aggregation
 - View current settings
 - Create new group
 - Enable/Disable
 - Restart
 - Delete configuration
 - Configure failover policy
- Versioning
 - Show Version Information

Chassis Configuration

ISS-2 (left)	ISS-2 (right)
Start ip address block: 10.105.130.10	Start ip address block: 10.105.132.10
End ip address block: 10.105.130.225	End ip address block: 10.105.132.225
Subnet Mask: 255.255.254.0	Subnet Mask: 255.255.254.0
☒ Default gateway: 10.105.130.1	☒ Default gateway: 10.105.132.1

Network

☒ Enable network time protocol

NTP Server 1: 10.105.5.26
NTP Server 2: 10.105.5.27

Date and Time

Current Time: Sun Dec 8 15:01:07 2013
Date (YYYY.MM.DD): YYYY.MM.DD
Time (HH.MM.SS): HH.MM.SS
Time Zone: GMT+11:00

Submit Reset

4. Do one of the following:

- ▶ To configure your system to use NTP to synchronize Storage Managers with a network reference, select Enable network time protocol, and then type the IP address of a primary NTP server. You can also type the IP address of a secondary NTP server.
- ▶ To set the time for a chassis manually, type the date and time in the Date and Time text boxes, and then select a time zone from the Time Zone menu.

5. Click Submit.

Resetting an Avid ISIS Engine to Factory Defaults

You can set the integrated switches back to the factory defaults. Resetting your configuration, including resetting the IP addresses of system components if your Avid ISIS system, can help correct some network communication problems.



Resetting switch configuration can lead to failed connectivity in your ISIS system and degrade performance. Reset your system only if directed to by Avid Customer Support personnel or under Avid Customer Support direction.

To reset an Avid ISIS Engine to its factory defaults:

1. Open the Switch Blade Agent for the Engine you want to reset. (For information on opening the Agent, see [“Avid ISIS | 7500 Switch Blade Agent” on page 155.](#))

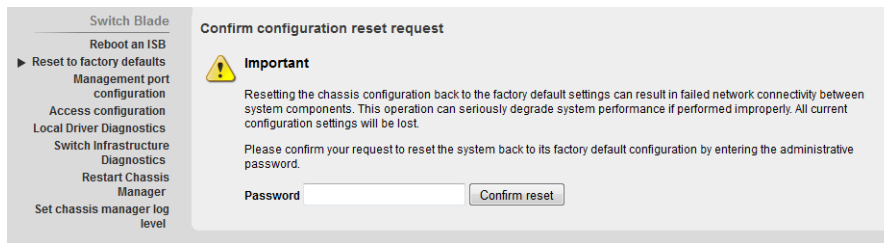
The Avid ISIS Integrated Ethernet Switch Blade Agent opens.

2. Click the Advanced tab.

The Advanced window opens.

3. Select “Reset to factory defaults” from the Switch Blade area.

A confirmation dialog box opens.



4. Type the Administrator password for your Avid ISIS system, and click Confirm reset.

The chassis switch configuration is reset to its factory defaults.

Switch Infrastructure Diagnostics

Avid ISIS supports system level diagnostics for every Avid ISIS switch from one location. The diagnostics organize results and provide a report of problems with the switch.

The Switch Diagnostics test does not fix diagnosed problems; instead, it looks for problems and provides clues as to the root cause. In many cases, the diagnostics can point to what the problem might be, where the problem is located, or how to address the problem. However, diagnostics cannot always determine the cause of the problem, and the test only reports relevant data for further analysis.

The diagnostic tests are organized into separate groupings. Each group investigates the switch in different ways to look for possible problems. If you are unsure if you have a problem or where a problem is, select all the test groups to get a more complete picture of the system's health. Each test exists in only one group. The following sections describe how the tests are arranged within the groups.

Stacking

The Stacking test group looks for symptoms of a problem with switch stack health. Run this group of tests if you think a switch is not properly stacked, or if you are having trouble with traffic flow on a particular switch.

Stack MAC Addresses

This is a report of MAC addresses for all Layer 2 visible switches in the stack from the reporting switch's perspective.

When the number of switches reported here is less than the number of switches reported by the Stack Serial Numbers Test, there could be problems reaching a switch that is supposed to be part of the stack. Sometimes this information can be verified by a failure in the Ping Stack Test. Or, if there is an extra switch listed in Stack Mac Addresses, it could mean that a switch is visible that is not yet part of the stack and may need to be added.

State Machine

When switches connect to each other to form a stack, they go through a state machine process. If the two switches have successfully completed their state machine process, they both reconcile to state STACKED. Switch Diagnostics will report any switches that have not reconciled to this state.



If Diagnostics is run immediately after connecting two switches together, then those switches might still be going through the normal state machine process and might not yet be reconciled. So, if Diagnostics is reporting an error in the State Machine Test, and the two switches were just connected, try waiting about 5 minutes and run Diagnostics again.

The following can result in problems reported in the State Machine Test:

- A Stack Collision prevents the State Machines from reconciling successfully. Check the results of the Collision Test.
- If another error has occurred during the State Machine Test, restart the process by disconnecting the stacking cable, and then reconnecting it. If the error persists, reboot the switch. If the error still persists, reboot both switches on either side of the stacking cable. Finally, try to reboot all switches on that side of the stack.

Stack Serial Numbers

This test reports the serial numbers of switches that are expected to be part of the stack from the reporting switch's perspective.

When the switches reported here are not the same as the switches reported by the Stack MAC Addresses Test, there could be problems reaching a switch that is supposed to be part of the stack. Sometimes this information can be verified by a failure in the Ping Stack Test.

The test can also report two chassis serial numbers with the same chassis ID (like an index). This could indicate a collision.

Module Assignment

This test makes sure that all switches have been assigned Module IDs correctly. This information is necessary for proper switch communication. If a problem is reported, your only option is to reboot the switch. If the problem persists, contact Avid Personnel for additional help.

Collision

Collisions result when two switches have conflicting configuration information. This can happen when connecting a new switch to a stack that has an IP address or chassis ID that conflicts with a switch that is already in the stack. To correct this, perform an "Add" from a switch that is already a part of the stack, and configure the new switch with non-conflicting information.

Performance

Link Aggregation Configuration

This test checks that Link Aggregation Configuration information is consistent among different processes in the switch. If a problem is reported here, try configuring link aggregation again through the switch Agent web page.

The test also checks each port that is a member of a link aggregation group to make sure that the link is up.

Link Aggregation Load Balancing

This test is marked informational. Therefore, no determination of PASS/WARN or FAILED will be made regarding the test result. In order to provide complete Link Aggregation Load Balancing results for the entire system, every switch that is a member of a link aggregation group must report information that is consistent with other switches in the system. If data is not consistent, or a result from a switch is missing, then the total data transmitted and received for all link aggregation groups cannot be determined. Review the data displayed carefully, and make sure that:

- The data transmitted and received is balanced between all port members of the link aggregation group. If system results are complete, then each port will report its percentage of data transmitted and received with regard to the total amount of data transmitted and received for that link aggregation group.
- If system results are not complete, then correct any other issues reported by Switch Diagnostics, and run Switch Diagnostics again.

Keep in mind how long link aggregation has been configured and how much load the system has been under. If link aggregation was just configured very recently, and there has not been much data load on the system, then the data reported may not provide you with applicable information. Make sure the system has been under load, and then run Diagnostics again to capture a new load balancing report.

Also, if one of the link aggregated port members has been down previously, then keep in mind that the data transmitted and received on this port will always be less than other group members (depending on how long this link was down). The data reported is a total of all packets sent and received on this port since the last time Switch Diagnostics was run.

The next time Diagnostics is run, the load balancing values will be cleared, so Download the Diagnostics results before running Diagnostics again in order for Avid Personnel to better analyze the situation.

Counters

Counters and Registers

When reviewing this data, keep in mind the last time these values were reset. Counters and incrementing Register values get reset every time the switch reboots or Diagnostics is run.



Some Register values under the “Registers” column cannot be cleared by Switch Diagnostics. These values can only be reset by rebooting the switch.

If the switch has been running for several months without running Diagnostics, then some of these values may get quite high, and still mean the system is healthy. Or, a spike of packet drops may have occurred several weeks in the past – so the values reported are high, but the network may have since cleared up. If values reported by Diagnostics seem suspect, and the system is still under data load, then try waiting a few minutes and run Diagnostics again. If the test still flags WARN or FAILED for values reported, then contact Avid Personnel for additional help.



The time to wait depends on how much system load is traveling through the switches, network configuration, how many clients are connected, etc.

Remember that the next time Diagnostics is run, the counter and register values will be cleared, so download the Diagnostics results before running Diagnostics again in order for Avid Personnel to better analyze the situation.

Connectivity

Default Gateway

If the gateway cannot be reached by ping, check the following:

- Is the gateway up and running?
- If there are switches between the storage system and the gateway, verify that every switch is running successfully and properly configured to allow communication to the gateway from the storage system.
- If there are switches between the storage system and the gateway, verify that the 10G link between the storage system and the switch has link (Port Link Information test) and is not dropping packets (Counters and Registers).

Ping Storage Blades

If a Storage Blade is not reachable by ping, make sure that the Storage Blade is not pulled out of its slot. If the Storage Blade appears to be seated, try reseating it. If the Storage Blade is still unreachable, try moving it to a different slot. If the LED lights up on the Storage Blade, then also check the Intermittent Link test for a possible intermittent link, and Counters and Registers for error statistics.

Ping Stack

If a member of the stack is not reachable, make sure the stacking cable to the problem switch is plugged in and has link at both ends. Check Hardware tests to be sure that the stacking link is not running at the wrong speed or suspected of having an intermittent link. Also, check test results in the Stacking test group in case there was a stacking error. Lastly, make sure Counters and Registers do not indicate errors have occurred on this stack port.

Hardware

Intermittent Link

An intermittent link is reported if the number of link ups or link downs on a port exceeds a predefined threshold. Keep the following in mind when viewing this report for the port that is reporting a possible intermittent link:

- Have you unplugged and plugged in a cable to this port several times since the last time Switch Diagnostics was run?
- If the port is for a Storage Blade, have you reseated this Storage Blade several times since the last time Switch Diagnostics was run? Has the Storage Blade rebooted several times since the last time Switch Diagnostics was run?
- If the port is for a client, have you rebooted this client several times since the last time Switch Diagnostics was run?

If you answered yes to any of the above, then these results do not necessarily indicate a hardware problem with the reported port or link. If there is no obvious explanation for the numerous link ups and link downs reported, there could be a hardware problem with the switch port, the cable, or the port on the other end (not the switch).

Intermittent Link statistics are cleared each time Diagnostics is run. To keep these results, download the Diagnostics results before running Diagnostics again.

Link Status

Whenever possible, Switch Diagnostics indicate ports that are down for ports that are supposed to be in use. All Storage Blades and all ports that are members of Link Aggregation groups are expected to have link. If they do not, they will be flagged within Switch Diagnostics as suspect. See Port Link Information for status on other ports.

Port Speeds

By default, client ports will not negotiate to any speed except 1000Mbps. Therefore, by default, if any client port was configured to run at a speed other than 1000Mbps, then link would not be established. If any client port is reporting a speed other than 1000Mbps, then it is possible that the default behavior was explicitly overridden. Do the following:

1. Configure the Client to run at 1000Mbps.
2. Reboot the switch.

Port Link Information

This test is marked informational. Therefore, no determination of PASS/WARN or FAILED will be made regarding the test result. This information is best used to compare a known topology (i.e. which stacking, 10G and client ports should be connected and working) to the displayed system link status for each reporting switch.

- **Client Ports**—Switch Diagnostics cannot determine whether a client port should have link or not – as this is specific to each setup. Therefore, use this information to make sure that the client ports in use are reporting link UP status as expected. Also, be aware that the switch will not negotiate to any speed except 1000Mbps on client ports. So, if a client is configured to run at a different speed, then the link will not be successfully established and will be reported as DOWN.
- **Stacking Ports**—Switch Diagnostics cannot determine in all cases whether a stack port should have link or not. Use this information to make sure that the stack ports in use are reporting link UP status as expected.
- **10G Ports**—Unless a 10G Port is part of a Link Aggregation Group, Switch Diagnostics cannot determine if this port should have link or not. Use this information to make sure that the 10G ports in use are reporting link UP status as expected.

Advanced

Unicast Bitmaps

This information indicates errors with the way traffic is mapped to stack ports. Avid Personnel will review this information.

Environment

Installation Errors

Switch Diagnostics indicates any installation failures reported on the switches. If an installation failure is reported, navigate to the Agent page on the switch reporting the failure and investigate the installation logs.

Processes

There are several important processes that need to run in order to achieve and maintain both switch and stack health. Switch Diagnostics will report any processes in a suspect state.

Running Switch Infrastructure Diagnostics

The diagnostics should not be used during a critical time in your production. Some tests burden system bandwidth and resources.

To access Switch Infrastructure Diagnostics:

1. In the Avid ISIS Switch Blade Agent, click the Advanced tab, then click Switch Infrastructure Diagnostics in the Switch Blade section of the command menu.
2. In the Run Switch Diagnostics dialog box, select the tests you want to perform.
3. In the Select network section, select the VLAN subnets you want to test:
 - Left
 - Right
 - Both
4. Click the Select chassis menu, and do one of the following:

- ▶ Select a chassis on which to run the diagnostics.
 - ▶ Select All to run the diagnostics on all chassis.
5. Click Run diagnostics.
- A progress bar appears as the diagnostics run. When the results are available, they are displayed in results window in table format. Each component is displayed in a separate row.
6. Click “View the Switch Diagnostics Results Summary Page.”
- The Switch Diagnostics Results Summary window opens.
7. When the Results Summary page is displayed, you can do one or more of the following:
- Click a column header to display detailed results for the selected group on all switches.
 - Click a switch to display detailed results for all groups on the selected switch.
 - Return to the Reported Results/System Overview Page.
 - View the Raw diagnostic output.
 - Download the result files to the local system.

Detailed results provide other display options. Each window includes instructions on how to view your results. For additional information, see the Switch Diagnostic Help link in the upper right corner of the window.

Switch Diagnostics Results

When using the Switch Infrastructure Diagnostics:

- Once the diagnostics have run on the selected tests, you can use the Switch Diagnostic Help link located in the upper right corner of the Reported Result window to read what each test performs and see appropriate solutions to any failed tests (see “Running Switch Infrastructure Diagnostics” on page 167).
- Brief instructions are displayed at the bottom of each display. Other statistic information is usually listed in table format after the results are available.
- After selecting the type of test to perform, you can then select a column in the display to select a particular test on a group of components or select a row to run all tests on just one component.

The results are displayed in these colors:

	Green	Passed
	Yellow	Warning. There is not enough information to confirm that the switch is in an error state; however, the test diagnostics has flagged a situation that might need attention. Double-click the warning text to display a list of possible reasons for the warning. For example, if a Storage Blade is pulled out, the ping test provides a warning result to inform you that the ping test failed. But the Storage Blade might have been intentionally pulled out, so it is an unknown condition and not a failure condition.
	Red	Failed. Double-click the failed text to display a list of possible reasons for the failure.
	Gray	This test was not selected to be performed.

Switch Blade Logging

The Logging tab provides a complete view of the logs of active switches. The logs provide you with a system snapshot that you can use to view error and status messages. The logs provide detailed status information that is especially useful to Avid Customer Support personnel for monitoring system status during prolonged operations.

For more information on the Logging tab, see the following topics:

- [Using Agent Logging](#)
- [Viewing Agent Event Logs](#)
- [Clearing Agent Event Logs](#)

Using Agent Logging

You can use the Logging tab to view event logs and to clear existing logs. The Logging tab contains two sections:

- Options area: the left area allows you to select specific logging options to display and to perform administrative tasks relating to the Agent logs.



The Kernel Ring Buffer displays logs maintained by the Linux kernel. These logs are used by Avid Customer Support.

- Logs area: the right area displays different types of events and information from the network component.

To access Agent Logging functions:

1. Open the Agent. (For information on opening the Agent, see [“Avid ISIS | 7500 Switch Blade Agent” on page 155.](#))
2. Click the Logging tab.

The Logging window opens.

Viewing Agent Event Logs

To view event logs:

1. Open the Agent. (For information on opening the Agent, see [“Avid ISIS | 7500 Switch Blade Agent” on page 155.](#))
2. Click the Logging tab.
The Logging window opens.
3. In the “Entries to view” text box, type the number of events to display. The default is 100. To view all events, type 0 (zero).
4. Select a log from the “Log to view” list.
5. Click View.

The event log displays in the Logs area.

Clearing Agent Event Logs

You can clear the logs in any of the logging categories. This empties the log of all event entries and resets the logging process.

To clear logs:

1. Open the Agent. (For information on opening the Agent, see [“Avid ISIS | 7500 Switch Blade Agent” on page 155.](#))
2. Click the Logging tab.
The Logging window opens.
3. Select a log from the “Log to clear” list.
4. Click Clear.
5. Click OK.

The event log is cleared, and logging is reset to start recording new events.

C Avid ISIS SNMP MIB Reference

A MIB (Management Information Base) is a virtual database that describes the objects available from the managed device. Using this information with your NMS (Network Management System), you can send queries, receive SNMP trap broadcasts, and configure notifications and alarms based on Avid ISIS System Director events.

Most NMS applications provide the ability to import MIB files. You can find the Avid ISIS System Director MIB at the following location:

D:\Program Files\Avid\ISIS System Director\ISIS.mib

The following table lists the values found within the Avid ISIS SNMP MIB.

Object	OID	Description
product		
ISIS_ProductName	.1.3.6.1.4.1.526.20.1.1	This variable shows the name of the ISIS product line.
ISIS_Version	.1.3.6.1.4.1.526.20.1.2	This variable shows the version of the ISIS install.
status		
ISIS_SystemDirectorState	.1.3.6.1.4.1.526.20.2.1	This variable shows the state of the System Director. • 0=Online • 1=Offline • 2=Standby • 3=Unknown
ISIS_SystemDirectorStateString	.1.3.6.1.4.1.526.20.2.2	This variable shows the state of the System Director in string format.
ISIS_CheckEventLog	.1.3.6.1.4.1.526.20.2.3	This variable shows whether the check event log flag is set.
ISIS_WorkspaceRedistributingCount	.1.3.6.1.4.1.526.20.2.4	This variable shows the current number of workspaces currently performing a redistribution.
performance		
ISIS_MegabytesPerSecond	.1.3.6.1.4.1.526.20.3.1	This variable shows total megabytes per second for all connected clients.
ISIS_ReadMegabytesPerSecond	.1.3.6.1.4.1.526.20.3.2	This variable shows total read megabytes per second for all connected clients.
ISIS_WriteMegabytesPerSecond	.1.3.6.1.4.1.526.20.3.3	This variable shows total write megabytes per second for all connected clients.
ISIS_MessagesPerSecond	.1.3.6.1.4.1.526.20.3.4	This variable shows the number of messages per second the System Director is processing.

Object (Continued)	OID	Description (Continued)
ISIS_OpenFiles	.1.3.6.1.4.1.526.20.3.5	This variable shows how many open files are currently open.
ISIS_ActiveClientCount	.1.3.6.1.4.1.526.20.3.6	This variable shows the active client count.
ISIS_MaximumClientCount	.1.3.6.1.4.1.526.20.3.7	This variable shows the maximum active client count.
usage		
ISIS_HighestDiskUsedPercentage	.1.3.6.1.4.1.526.20.4.1	This variable shows the highest percent used across all disks.
ISIS_TotalSystemMB	.1.3.6.1.4.1.526.20.4.2	This variable shows how total system megabytes.
ISIS_TotalAllocatedMB	.1.3.6.1.4.1.526.20.4.3	This variable shows how total allocated megabytes. Allocated size is the sum of all the workspace sizes.
ISIS_TotalUsedMB	.1.3.6.1.4.1.526.20.4.4	This variable shows the total system usage across all workspaces.
ISIS_FileCount	.1.3.6.1.4.1.526.20.4.5	This variable shows the total number of files across all workspaces.
ISIS_FolderCount	.1.3.6.1.4.1.526.20.4.6	This variable shows the number of folders across all workspaces.
ISIS_WorkspaceCount	.1.3.6.1.4.1.526.20.4.7	This variable shows the total number of workspaces.

D Avid ISIS E-mail Notification List

The following table lists the events logged by the System Director Service and related components, and a brief description of what the error means. This list does not include the administrator server service.

In this table, %s represents a string, such as an object name, and %d represents a numeric value. The actual error messages in the event log will contain the name or value of the subsystem that generated the error.

Subcode	Severity	ISIS Infrastructure	Message
ISIS General	Information	All	Administrator password reset was requested by administrative command
ISIS General	Information	7500	ISIS chassis SN %s : Power supply < %d > present
ISIS General	Information	7500	ISIS chassis SN %s : Power supply < %d > DC OKAY
ISIS General	Information	All	Storage Element remove scheduled
ISIS General	Information	All	%s completed for < %s >
ISIS General	Information	All	%s started for < %s >
ISIS General	Warning	All	Workspace < %s > free space at or below warning threshold
ISIS General	Warning	All	Client %s is being forced to disconnect by an administrative command
ISIS General	Warning	All	Deleting Workspace < %s >
ISIS General	Warning	All	Canceling delete Workspace < %s >
ISIS General	Warning	All	< %s > has reached the config depth warning threshold
ISIS General	Warning	All	%s suspended for < %s >
ISIS General	Error	All	Workspace < %s > is full\n
ISIS General	Error	All	Workspace < %s > free space at or below critical threshold\n
ISIS General	Error	All	Avid ISIS dongle was not found. Clients may not be allowed to connect.
ISIS General	Error	All	Avid ISIS dongle version is incorrect. Clients may not be allowed to connect.
ISIS General	Error	7500	ISIS chassis SN %s : Power supply < %d > not present
ISIS General	Error	7500	ISIS chassis SN %s : Power supply < %d > DC not OKAY
ISIS General	Error	All	< %s > has reached the config depth critical threshold
ISIS General	Error	All	< %s > scheduled for full rebuild. Depth is %d

Subcode	Severity	ISIS Infrastructure	Message (Continued)
ISIS General	Error	All	“Removing failed Storage Element %s, unit < %d, %d >, sn %s chassis %s, slot %d”
ISIS General	Error	All	Storage Element remove not scheduled, status %d
ISIS General	Error	All	%s completed in error for < %s >
ISIS General	Error	All	SE%03d failed to complete %s
ISIS General	Success	All	Install File System Successful, Meta Data is %d MB
ISIS General	Error	5500	ISIS Storage Engine <hostname>: CMOS battery fault detected
ISIS General	Information	5500	ISIS Storage Engine <hostname>: CMOS battery fault cleared
ISIS General	Error	5500	ISIS Storage Engine <hostname>: Processor Over Temperature fault detected
ISIS General	Information	5500	ISIS Storage Engine <hostname>: Processor Over Temperature fault cleared
ISIS General	Error	5500	ISIS Storage Engine <hostname>: Power-supply fault detected
ISIS General	Information	5500	ISIS Storage Engine <hostname>: Power-supply fault cleared
ISIS General	Error	5500	ISIS Storage Engine <hostname>: Engine Over Temperature fault detected
ISIS General	Information	5500	ISIS Storage Engine <hostname>: Engine Over Temperature fault cleared
ISIS General	Error	5500	ISIS Storage Engine <hostname>: Fan fault detected
ISIS General	Information	5500	ISIS Storage Engine <hostname>: Fan fault cleared
ISIS General	Error	5500	ISIS Storage Engine <hostname>: System drive fault detected
ISIS General	Information	5500	ISIS Storage Engine <hostname>: System drive fault cleared
ISIS General	Error	7500 5500	ISIS Storage Engine <hostname>: Software fault detected
ISIS General	Error	7500 5500	ISIS Storage Engine <hostname>: Network adapter settings error detected
Server Control	Information	All	Avid ISIS System Director service stopped.
Server Control	Information	All	System Director service can not be started (err = %ld)
Server Control	Information	All	Interactive Start of System Director
Server Control	Information	All	Avid System Director (Version %s) has successfully started
Server Control	Error	All	System Director service can not be started (err = %ld)
Server Control	Error	All	Server will not start with an incorrect time setting.
Server Control	Error	All	There is a problem saving metadata. Shutting down.
Storage Blade General	Information	7500	Storage Element %s, unit <%d,%d>, SN %s, chassis %s, slot %d: Repairing mirrors completed

Subcode	Severity	ISIS Infrastructure	Message (Continued)
Storage Blade General	Information	7500 5500	Storage Element %, unit <%d,%d>, SN %, chassis %, slot %d: Disk performance no longer degraded
Storage Blade General	Information	7500 5500	Storage Element %, unit <%d,%d>, SN %, chassis %, slot %d: Disk no longer full
Storage Blade General	Information	7500 5500	Storage Element %, unit <%d,%d>, SN %, chassis %, slot %d: Network no longer degraded
Storage Blade General	Information	7500 5500	Storage Element %, unit <%d,%d>, SN %, chassis %, slot %d: Temp normal
Storage Blade General	Information	7500 5500	Storage Element %, unit <%d,%d>, SN %, chassis %, slot %d: Reconnected
Storage Blade General	Warning	7500 5500	Storage Element %, unit <%d,%d>, SN %, chassis %, slot %d: Disks under test
Storage Blade General	Warning	7500 5500	Server %, SN %, chassis %, slot %d: Send unbind because not current member
Storage Blade General	Warning	7500 5500	Storage Element %, unit <%d,%d>, SN %, chassis %, slot %d: No connection
Storage Blade General	Warning	7500 5500	Can not add < %s > : microserver has incompatible version
Storage Blade General	Error	7500	Storage Element %, unit <%d,%d>, SN %, chassis %, slot %d: Repairing mirrors
Storage Blade General	Error	7500 5500	Storage Element %, unit <%d,%d>, SN %, chassis %, slot %d: Disks failed
Storage Blade General	Error	7500 5500	Storage Element %, unit <%d,%d>, SN %, chassis %, slot %d: Disk performance degraded
Storage Blade General	Error	7500 5500	Storage Element %, unit <%d,%d>, SN %, chassis %, slot %d: Memory error
Storage Blade General	Error	7500 5500	Storage Element %, unit <%d,%d>, SN %, chassis %, slot %d: Disk full
Storage Blade General	Error	7500 5500	Storage Element %, unit <%d,%d>, SN %, chassis %, slot %d: Metadata errors
Storage Blade General	Error	7500 5500	Storage Element %, unit <%d,%d>, SN %, chassis %, slot %d: Network degraded
Storage Blade General	Error	7500 5500	Storage Element %, unit <%d,%d>, SN %, chassis %, slot %d: Temp critical
Storage Blade General	Error	7500 5500	Storage Element %, unit <%d,%d>, SN %, chassis %, slot %d: Temp warning
Storage Blade General	Error	All	Remove failed because: Workspace reservations exceed capacity
Storage Blade General	Error	All	Remove failed because: Would be too few Storage Elements

Subcode	Severity	ISIS Infrastructure	Message (Continued)
Storage Blade General	Error	All	Remove failed because: Already removed
Storage Blade General	Error	All	Storage Element remove not scheduled - too many errors
Storage Blade General	Error	All	Storage Element remove not scheduled - servers not connected
Switch Blade General	Information	7500	ISIS chassis SN %s : Status reported from switch in slot %d
Switch Blade General	Information	7500	ISIS chassis SN %s, Switch slot %d : Temp normal
Switch Blade General	Error	7500	ISIS chassis SN %s, Switch slot %d : No status reported
Switch Blade General	Error	7500	ISIS chassis SN %s, Switch slot %d : Temp critical
Switch Blade General	Error	7500	ISIS chassis SN %s, Switch slot %d : Temp warning
Switch Blade General	Error	7500	ISIS chassis SN %s, Switch slot %d : Stacking alert
Switch Blade General	Error	7500	ISIS chassis SN %s, Switch slot %d : Trunking alert
Switch Blade General	Error	7500	ISIS chassis SN %s, Switch slot %d : Chassis alert
Switch Blade General	Error	7500	"ISIS chassis SN %s, Switch slot %d : Unspecified alert
Switch Blade General	Error	7500	ISIS chassis SN %s, Switch slot %d : Link alert, HiG or 10Gig
Switch Blade General	Error	7500	ISIS chassis SN %s, Switch slot %d : Memory (ECC) alert
Switch Blade General	Error	7500	ISIS chassis SN %s, Switch slot %d : Driver compatibility alert
Switch Blade General	Error	7500	ISIS chassis SN %s, Switch slot %d : Security disabled alert
System Director	Information	All	Cannot locate valid metadata to load
System Director	Information	All	Loading metadata from %s
System Director	Information	All	Metadata converter generated new export file
System Director	Information	All	Memory size changed. File system can be reconfigured
System Director	Information	All	Partition does not fit into server configured memory. Available memory is too small.
System Director	Information	All	Export started
System Director	Information	All	Export complete
System Director	Information	All	Export did not complete
System Director	Information	All	Unmount Partition
System Director	Information	All	Reconfiguring because of install file system request
System Director	Information	All	Updated tiebreaker IP address (%d): %s
System Director	Information	All	System Director was requested to force clients to log out
System Director	Information	All	Offline Canceled
System Director	Information	All	MetaUpgrade: Validated PartitionDump.bin file
System Director	Information	All	MetaUpgrade: Starting %s metadata converter

Subcode	Severity	ISIS Infrastructure	Message (Continued)
System Director	Information	All	Server start is scheduled in non-redundant configuration
System Director	Information	All	This server became the primary System Director due to a Dual System Director event.
System Director	Information	All	This server is ready to become the primary System Director because it was the last active server.
System Director	Information	All	Remote System Director is already active - enabling synchronization
System Director	Information	All	This server became the primary System Director because other system is new standby.
System Director	Information	All	This server became the primary System Director because it was the most recent metadata.
System Director	Information	All	This server became the active System Director because it had the same version as the other server.
System Director	Information	All	The other server has more recent metadata - enabling synchronization
System Director	Information	All	The metadata server is not in agreement - disregarding
System Director	Information	All	This server now the active System Director.
System Director	Information	All	Started IP address %s on interface %s
System Director	Information	All	Could not find an interface with IP address %s
System Director	Information	All	Unable to start Dual System Director IP address %s
System Director	Information	All	Unable to start IP address %s :
System Director	Information	All	Dual System Director IP address %d is not configured or enabled
System Director	Information	All	Saved %s to %s
System Director	Information	All	Metadata conversion earlier than BASE_VERSION_V28 not supported
System Director	Information	All	Metadata conversion from metadata version %d not supported
System Director	Information	All	Metadata upgrade completed.
System Director	Information	All	validateFS(): warning, fix made to allocated byte counts
System Director	Information	All	validateFS(): warning, fix made to byte counts
System Director	Warning	All	Failed to setup a Metadata save operation for %s
System Director	Warning	All	Unable to clear previous tiebreaker IP address: fstatus %d
System Director	Warning	All	Unable to update tiebreaker IP address: fstatus %d
System Director	Warning	All	No export file to save. Metadata upgrade will continue.
System Director	Warning	All	Start metadata create failed status = %d

Subcode	Severity	ISIS Infrastructure	Message (Continued)
System Director	Warning	All	Metadata create wait failed, status = %d, state = %d
System Director	Warning	All	Metadata create failed
System Director	Warning	All	Start metadata load failed
System Director	Warning	All	Metadata load wait failed, status = %d, state = %d
System Director	Warning	All	Metadata load failed
System Director	Warning	All	Metadata load wait failed, status = %d, state = %d
System Director	Warning	All	Metadata is being deleted by user instruction
System Director	Warning	All	Free space on C: has dropped below 11GB
System Director	Warning	All	Free space on C: has dropped below 26GB
System Director	Error	All	FSrespond failed. Status is: %d
System Director	Error	All	Unable to validate PartitionDump.bin that was just created
System Director	Error	All	Import pass 2: could not reconstruct from the import file
System Director	Error	All	THE IMPORT FAILED PLEASE CALL AVID SERVICE BEFORE DOING ANYTHING ELSE
System Director	Error	All	Failed to allocate memory error = %d
System Director	Error	All	Metadata converter failed to generate export file
System Director	Error	All	Metadata import failed - file mgr exiting - call AVID support
System Director	Error	All	Dismount failed. Partition did not validate
System Director	Error	All	Unable to save metadata to %s sequence number ""INT64_FORMAT""
System Director	Error	All	Going to fail Install File System, Memory Needed %d, Avail %d
System Director	Error	All	Failed to create a unique id
System Director	Error	All	Failed to create root Storage Element set
System Director	Error	All	Local drive does not contain enough free space for meta data files
System Director	Error	All	*****THE INSTALL FILESYSTEM FAILED ***** fs error %d
System Director	Error	7500 5500	Synchronization metadata did not verify
System Director	Error	All	Meta data is corrupted
System Director	Error	7500 5500	checkForMetaDataSave() sending to standby server is taking too long to complete
System Director	Error	7500 5500	checkForMetaDataSave() saving to a file is taking too long complete

Subcode	Severity	ISIS Infrastructure	Message (Continued)
System Director	Error	All	Failed to update metadata on %s
System Director	Error	All	Severe disk errors, must shut down now
System Director	Error	7500 5500	CSMetaDataSendDone - the checksum engine may be stuck
System Director	Error	7500 5500	sendMetaSyncToStandby() An async request is taking too long to complete
System Director	Error	7500 5500	sendMetaSyncToStandby() replication is taking too long to complete
System Director	Error	All	Local drive does not contain enough free space for meta data file
System Director	Error	All	Unable to open a local metadata file
System Director	Error	All	The low priority scheduler seems hung. Shutting down.
System Director	Error	All	Assert Error from %s line %d, %s
System Director	Error	All	Server shutdown
System Director	Error	All	MetaUpgrade: Metadata converter (%s) was not present
System Director	Error	All	MetaUpgrade: Error starting for metadata converter - err %d
System Director	Error	All	MetaUpgrade: Error waiting for metadata converter - err %d
System Director	Error	All	MetaUpgrade: Error obtaining metadata converter exit status - err %d
System Director	Error	All	Metadata copy seems out of date so this system will not become active.
System Director	Error	All	System Director shutting down because standby server may have better connectivity
System Director	Error	All	Failed to save %s to %s
System Director	Error	All	Export file not saved. Metadata upgrade will not continue.
System Director	Error	All	Metadata upgrade starting.
System Director	Error	All	Free space on C: has dropped below 6GB
System Director	Error	All	Free space on D: has dropped below 16GB
System Director	Success	All	MetaUpgrade: Metadata conversion completed by %s
System Director	Success	All	MetaUpgrade: Metadata conversion was not completed by %s

ISIS | 5500 Media Drive LED Functions

This section describes the ISIS | 5500 media drive LED functions. Each media drive has a blue and red LED on the bottom front of the drive. The left LED (blue) is on when a drive has power and flashes when the drive is in use. The right LED (red) is lit when an error is detected with the drive and the drive needs to be replaced. Details on the media drive LED indicators are in the following table.



The following media drive LED functions have changed for systems with the 6 Gb SAS expander board. These changes have been incorporated into Engine shipments starting in September 2011.

6 Gb SAS Expander — Media Drive LED Functions

Drive State	Blue LED	Red LED	Management Console Messaging	Comments
Online Inactive	On solid	Off	No Special Status	Healthy online drive, no disk I/O
On-line Active	Activity	Off	No Special Status	Healthy online drive, with disk I/O
Healthy Spare	On solid	Off	No Special Status	Healthy Global Hot Spare disk
Online Disk in a Degraded Set	On solid/ Activity	Fast flashing	Error – Disk Performance Degraded	Nothing needs to be done to these online drives, but failed drive should be replaced
Spare Rebuilding	Activity	Slow flashing	Error – Disk Performance Degraded – Rebuilding x%	Rebuild automatically occurs on drive failure by using Hot Spare disk
Data Rebuilding	Activity	Fast flashing	Error – Disk Performance Degraded – Rebuilding x%	Rebuild automatically occurs on drive failure by using Hot Spare disk
Consistency Check	Activity	Off	Checking Raid Set – x%	No user intervention required
Initializing	Activity	Off	Initializing Raid Set – x%	Happens on initial array creation
Failed Data Disk	On solid	On solid	Error – Disk Performance Degraded	Should replace disk
Failed Spare Disk	On solid	On solid	Missing Spare	Should replace disk
Unused Disk	On solid	Off	No Special Status	No user intervention required
Non-Branded	On solid	Slow flashing	Warning – Unapproved spare disk attempting to be added as a hot spare	Should replace disk

3 Gb SAS Expander — Media Drive LED Functions

Drive State	Blue LED	Red LED	Management Console Messaging	Comments
On-line Inactive	On solid	Off	No Special Status	Healthy online drive, no disk I/O
On-line Active	Activity	Off	No Special Status	Healthy online drive, with disk I/O
Healthy Spare	On solid	Slow flashing	No Special Status	
Online Disk in a Failed Set	On solid/Activity	Double flashing	Error – Disk Performance Degraded	Nothing needs to be done to these online drives, but failed drive should be replaced
Spare Rebuilding	Activity	Activity	Error – Disk Performance Degraded – Rebuilding x%	Automatically occurs on drive failure
Data Rebuilding	Activity	Double flashing	Error – Disk Performance Degraded – Rebuilding x%	Automatically occurs on drive failure
Consistency Check	Activity	Fast flashing	Checking Raid Set – x%	No user intervention required
Initializing	Activity	Fast flashing	Initializing Raid Set – x%	Happens on initial array creation
Failed Data Disk	On solid	On solid	Error – Disk Performance Degraded	Should replace disk
Failed Spare Disk	On solid	On solid	Missing Spare	Should replace disk
Unused Disk	On solid	Off		
Non-Branded	Medium Flashing	Off	Warning – Unapproved spare disk attempting to be added as a hot spare	Should replace disk

Index

A

- Access privileges
 - considerations [80](#)
 - duplicating users [94](#)
 - effective [80](#)
 - managing [80](#)
 - new users [94](#)
 - Workspace, setting [81](#)
- Account Synchronizer (LDAP Sync tool) [101](#)
- Accounts
 - See* User accounts, User group accounts, Device accounts
- Active clients
 - checking license status [60](#)
 - disconnecting [60](#)
 - managing [59](#)
 - obsolete entries [60](#)
 - See also* Bandwidth tool
- Active Clients tab (System Director Control Panel) [54](#)
 - checking license status [60](#)
 - described [59](#)
 - disconnecting client [60](#)
 - obsolete entries [60](#)
- Activity LED [180](#)
- Adding
 - Device accounts [107](#)
 - LDAP/Active Directory groups [102](#)
 - Storage Groups [65](#)
 - Storage Managers [38, 40](#)
 - Storage Managers (to Storage Groups) [65](#)
 - user groups [98](#)
 - Users [93](#)
 - Workspaces [74](#)
- Administration Logs
 - described [23, 118](#)
 - downloading [118](#)
 - filtering [118](#)
 - tool [23](#)
 - viewing [118](#)
- Administration tool
 - See* Management Console
- Administrator password (Management Console)
 - resetting (System Director Control Panel) [59](#)
 - setting/changing [29](#)
- Administrator password (Storage Manager Agent)
 - default [149](#)
 - setting/changing [149](#)
- Administrator Password tool (Management Console) [23](#)
- Advanced Settings tab (System Director Control Panel)
 - metadata dump text file (PartitionDump.txt) [58](#)
 - resetting ISIS Administrator password [59](#)
- Advanced tab (Avid ISIS Agents) [160](#)
- Advanced Workspaces Commands [85](#)
- Agents
 - clearing logs [169](#)
 - configuration values [157](#)
 - described [155](#)
 - diagnostic tools [163](#)
 - ISIS 5500
 - ISIS 7500
 - link aggregation [157](#)
 - logging [169](#)
 - Logging tab [160, 169, 169](#)
 - logging window [169](#)
 - options [139](#)
 - Statistics tab [159](#)
 - System tab [157](#)
 - Tools tab [159](#)
 - Trace Setup tool [23](#)
 - user interface overview [155](#)
 - viewing logs [169](#)
- Aggregate logs [125, 125, 129](#)
 - options [126](#)
- Allocating Workspaces [71, 76](#)
- Auto Refresh
 - enabling and disablingSession, preventing timeout [25](#)
- Auto-Rectify [29](#)
 - default value [28](#)
 - Management Console preferences [28](#)
- Avid
 - online support [13](#)
 - training services [13](#)
- Avid ISIS
 - connected clients limit [90](#)
 - logging [118](#)
 - monitoring and diagnostics [115](#)
 - user accounts limit [90](#)

- user group accounts limit 90
- Avid ISIS Engine
 - resetting to factory defaults 160, 162
- Avid ISIS Help
 - See Help
- Avid ISIS Launch Pad
 - See ISIS Launch Pad
- Avid ISIS Management Console
 - See Management Console
- Avid ISIS Switch Manager
 - See Switch Manager tool
- Avid ISIS System Director
 - See System Director
- Avid ISIS System Director Control Panel
 - See System Director Control Panel

B

- Bandwidth
 - aggregate 110
 - monitoring 110
 - reservations 113
 - monitoring 113
 - revoking 114
 - system 110
- Bandwidth tool
 - See also active clients
 - described 22, 110, 111, 114
 - opening 111
 - revoking bandwidth reservations 114
 - scaling bandwidth graph display 111
- Blade Identification view (System Monitor tool) 138
- Buttons, Launch Pad 51

C

- Changing System Director virtual name 55
- Chassis
 - descriptions 46
 - Details panel 46
- Checking active client license status 60
- Chunk size
 - and Workspaces 71
 - matching to file system 64
- Clear Foreign Configuration 148
- Clearing
 - foreign disk 148
 - LDAP Sync tool History log 104
 - Network Degraded status messages 39
 - status event history 123
 - Storage Manager Agent logs 151
 - system logs 119
- Client accounts
 - described 90
 - See also User accounts, User group accounts, Device accounts
- Closing
 - Groups tool Details panel 97

- LDAP Sync tool 104
- Log Aggregator tool 126
- Retrieve Storage Manager Parameters 129
- Storage Groups tool Details panel 62
- Storage Managers tool Details panel 35
- Users tool User Details panel 92
- Workspaces tool Details panel 73
- Collapsing the Launch Pad 51
- Columns (LDAP Sync tool)
 - resizing 101
 - sorting 101
- Columns (Management Console)
 - moving 23
 - showing and hiding 24
 - sorting 24
 - sorting (multi-level) 24
- Concurrent Retrieval Threads 126
- Configuration tab (System Director Control Panel) 55
 - changing System Director virtual name 55
 - creating file system 57
 - opening Memory Log Viewer 52, 56
 - reconfiguring file system 57
 - System Director Memory Log Viewer 56
- Configuration values for Agents 157
- Configuring
 - contact information (Notification service) 32
 - general settings (System Director) 55
 - Management Console 28
- Connecting to servers (LDAP Sync tool) 105
- Connection Analyzer tool
 - See also ISIS Toolbox
 - checking connection status 124
 - described 123
 - opening 124
 - status icons 124
- Connection Status tool
 - described 22, 111, 112
 - disconnecting clients 113
 - opening 112
- Connections, managing 110
- Contact information (Notification service) 32
- Context menus (Management Console) 26
- Control Panel
 - See System Director Control Panel
- Creating
 - agent profiles 148
 - aggregate logs 126, 126
 - device accounts 107
 - ISIS file system 57
 - ISIS snapshot 120
 - ISIS snapshot archives 121
 - metadata dump text file (System Director Control Panel) 58
 - profiles 122
 - profiles (Management Console) 122
 - profiles (Storage Manager Agent) 148
 - snapshots 121
 - snapshots 120

- Storage Groups [65](#)
- System Director file system [57](#)
- user accounts [93](#)
- user group accounts [98](#)
- Workspaces [74](#)

D

- Data protection
 - mirrored
 - required Storage Managers [71](#)
 - RAID-6
 - chunk size [71](#)
 - required Storage Managers [71](#)
- Date, changing on chassis switch [158](#)
- Default Bandwidth for Auto Created Devices (Management Console preferences) [28](#)
 - default value [28](#)
- Default Hard Disk Error Threshold (Management Console preferences) [28](#)
 - default value [28](#)
- Default LCT Threshold [28](#)
- Default password
 - Management Console [15](#)
 - Storage Manager Agent [149](#)
- Delete log save location [29](#)
- Delete Logging (Management Console preferences) [28](#)
 - default value [28](#)
- Deleting
 - agent profiles [149](#)
 - all ISIS snapshots [121](#)
 - all profiles (Management Console) [122](#)
 - client accounts [108](#)
 - Device accounts [108](#)
 - ISIS snapshot [121](#)
 - ISIS snapshot archives [121](#)
 - profiles (Management Console) [122](#)
 - RAID sets [148](#)
 - Storage Groups [68](#)
 - Storage Manager Agent profiles [149](#)
 - Storage Manager Agent saved logs [152](#)
 - User accounts [95](#)
 - user group accounts [99](#)
 - Workspaces [79](#)
- Details
 - Engine [46](#)
 - Storage Managers [46](#)
 - Switches [46](#)
- Device accounts
 - See also* Client accounts
 - adding [107](#)
 - deleting [108](#)
 - managing [106](#)
 - modifying [108](#)
- Devices tool
 - adding Device accounts [107](#)
 - deleting Device accounts [108](#)
 - described [22](#), [106](#)
 - Details panel [107](#)
 - Device accounts list [107](#)
 - modifying Device accounts [108](#)
 - viewing Device account details [107](#)
- Diagnostic tests
 - results [168](#)
 - running Switch Infrastructure Diagnostics [167](#)
 - test groups [163](#)
- Diagnostic tools
 - Avid ISIS Agents [160](#)
 - Switch Manager tool [130](#)
- Disabling
 - Storage Manager logging [152](#)
 - User accounts [96](#)
- Disconnecting
 - client (System Director Control Panel) [60](#)
 - clients [113](#)
 - from LDAP server (LDAP Sync tool) [105](#)
- Disk Analyzer tool
 - described [127](#)
 - disk test options [128](#)
 - opening [127](#)
 - running disk tests [128](#)
 - saving results [129](#)
 - Storage Manager statistics [127](#)
 - updating display [128](#)
- Disk S.M.A.R.T. (Self-Monitoring, Analysis, And Reporting Technology)
 - See* Disk Analyzer tool
- Disk, clearing foreign configuration [148](#)
- Documentation, online [13](#)
- Domain ID [158](#)
- Downloading
 - Administration Logs [118](#)
 - ISIS snapshot archives [121](#)
- Drive
 - carrier latch [180](#)
 - LED [180](#)
- Drive sets
 - See* Storage Managers
- Duplicating
 - user accounts [94](#)
 - Workspaces [75](#)

E

- Email notifications
 - See* Notification service
- Enabling Storage Manager logging [152](#)
- Engine page [45](#)
- Entering text (Management Console) [26](#)
- Error notification
 - configuring parameters (Notification service) [32](#)
 - Notification service [31](#)
- Event triggers
 - described [78](#)

- setting 78
- Expanding the Launch Pad 51
- External Authentication
 - configuring 30
 - described 30
 - See also* Avid LDAP Account Synchronizer
- External Authentication tool 23, 30

F

- Factory defaults, resetting 160, 162
- File system
 - creating 57
 - matching chunk size of ISBs 64
 - operations (System Director) 56
 - reconfiguring 57
- Filtering
 - Administration logs 118
 - information (Management Console) 24
 - limitations (Management Console) 25
 - resetting (Management Console) 25
- Force Manual Device Creation (Management Console preferences) 28, 28

G

- General Configuration Options dialog box 55
- General settings (System Director) 55
- General view (System Monitor tool) 136
- Groups tool
 - closing Details panel 97
 - described 22, 96
 - hiding user membership panel 97
 - hiding Workspace Access panel 97
 - modifying accounts 98
 - user membership panel 97
 - viewing group details 97
 - Workspace Access panel 97

H

- Hard drive
 - See* Drive
- Hardware, managing 33
- Help
 - accessing 20
 - menu 20
- Hiding
 - Groups tool user membership panel 97
 - Groups tool Workspace Access panel 97
 - Users tool Details panel 92
- History Data Collection (Management Console preferences) 28
 - default value 28

I

- Illegal characters (Management Console) 26
- Importing incorrectly formatted UUIDs (LDAP/AD) 104
- Installers tool 22
- ISB, matching chunk size to file system 64
- ISIS | 7500 System Monitor tool 39
- ISIS Launch Pad
 - buttons 51
 - described 49
 - opening 50
 - opening Management Console 50, 51, 51
 - Storage Manager Viewer 52
- ISIS Management Console
 - Avid ISIS Agents 155
 - See* Management Console
- ISIS Notification service
 - See* Notification service
- ISIS Snapshots tool
 - collected information 120
 - creating ISIS snapshot archives 121
 - creating snapshot 120
 - deleting ISIS snapshot 121
 - deleting ISIS snapshot archives 121
 - described 23, 120
 - downloading archives 121
 - file name format 120
 - ISIS snapshot archives 121
 - Log Aggregator tool 120
 - output format 120
 - snapshot archive file location 121
 - snapshot archive file name format 121
 - snapshot archives described 121
 - snapshot file location 120
 - using 120
- ISIS SNMP
 - described 139
 - ISIS 5500 MIB reference 171
 - ISIS events 139
 - MIB file location 139, 171
 - monitoring 139
- ISIS SubCodes
 - See* error notification parameters (Notification service)
- ISIS System Director
 - opening Memory Log Viewer 52, 56
 - virtual name conventions 55
- ISIS Toolbox
 - See also* Connection Analyzer tool
 - See also* Disk Analyzer tool
 - See also* Log Aggregator tool
 - described 123
 - opening 124, 125, 127
 - Storage Manager Parameters 129
- ISS modules
 - upgrading 44, 47, 47
- IXS modules
 - upgrading 44, 47, 47

L

- Launch Pad
 - collapsing and expanding [51](#)
- LDAP (Lightweight Directory Access Protocol)
 - external authentication [30](#)
 - remote LDAP users [30](#)
 - See also* LDAP Sync tool
- LDAP Sync tool
 - See also* External Authentication
 - account list and selections report [103](#)
 - Account Synchronizer [101](#)
 - adding LDAP/Active Directory groups [102](#)
 - clearing History log [104](#)
 - closing [104](#)
 - columns
 - resizing [101](#)
 - sorting [101](#)
 - compatibility [100](#)
 - connecting and disconnecting from servers [105](#)
 - described [99](#)
 - importing users with bad UUIDs [104](#)
 - installing [100](#)
 - login information storage [100](#)
 - modifying
 - display [101](#)
 - group reconciliation actions [103](#)
 - opening [100](#)
 - printing History log [104](#)
 - removing LDAP/Active Directory groups [103](#)
 - resizing columns [101](#)
 - sorting columns [101](#)
 - synchronization status icons [101](#)
 - synchronizing accounts [102](#)
 - synchronizing LDAP/Active Directory groups [104](#)
 - user list and selections report [103](#)
 - using [101](#)
 - viewing History log [104](#)
- LED
 - drive activity [180](#)
 - drive power [180](#), [180](#)
 - function [180](#)
- Link aggregation
 - Trunking [157](#)
- Log Aggregator tool
 - Administrative privileges [126](#)
 - aggregate log options [126](#)
 - closing [126](#), [130](#)
 - Concurrent Retrieval Threads (setting) [126](#)
 - creating aggregate logs [126](#)
 - described [125](#), [125](#), [129](#)
 - event logs [125](#), [129](#)
 - LSI [125](#)
 - opening [125](#)
 - output format [127](#)
 - using [125](#)
 - viewing aggregate logs [127](#)

- Logging tab (Avid ISIS Agents) [160](#), [169](#)

Logs

- administration [118](#)
- Agent logging [160](#), [169](#)
- aggregate [125](#), [125](#), [129](#)
- application [119](#)
- clearing Agent logs [169](#)
- security [119](#)
- Storage Manager [52](#), [150](#), [153](#)
- system (Management Console) [119](#)
- System Director [56](#)
- viewing Agent logs [169](#)

LSI Log Aggregator tool [125](#)

M

Management Console

- See also* Management Console tools
- Adobe® Flash® player [17](#)
- Auto Refresh [25](#)
- Auto-Rectify [29](#)
- Auto-Rectify (preferences) [28](#)
- configuring [28](#)
- configuring preferences [28](#)
- context menus [26](#)
- Default
 - LCT Threshold [28](#)
- default
 - Bandwidth for Auto Created Devices [28](#)
 - Hard Disk Error Threshold [28](#)
 - password [15](#)
- delete log [29](#)
- Delete Logging (preferences) [28](#)
- described [17](#)
- entering text [26](#), [26](#)
- filtering information [24](#), [25](#)
- Force Manual Device Creation (preferences) [28](#)
- Help menu [20](#)
- History Data Collection (preferences) [28](#)
- Home page [15](#)
- log in [16](#)
- log out [17](#)
- logging [118](#)
- moving columns [23](#)
- navigation toolbar [20](#)
- non-administrative login [15](#)
- opening (as Administrator) [16](#)
- organizing display information [23](#)
- password (default) [15](#)
- resetting Administrator password [59](#)
- selecting items [26](#)
- session counter [21](#)
- setting Administrator password [29](#)
- Show status before login (preferences) [28](#)
- showing and hiding columns [24](#)
- sorting information [24](#)

- Storage Manager Agent [141](#)
 - supported web browsers [15](#)
 - Switch Blade Agent [155](#)
 - System Status Console [17](#)
 - text guidelines [26](#)
 - tools overview [21](#)
 - Total System Bandwidth (preferences) [28](#)
 - updating information (refresh) [25](#)
 - using [17](#)
 - Management Console tools
 - Administration Logs tool [23](#), [118](#)
 - Administrator Password tool [23](#), [29](#)
 - Agent Options tool [139](#)
 - Agent Trace Setup tool [23](#), [139](#)
 - Bandwidth tool [22](#), [110](#), [110](#)
 - Connection Status tool [22](#), [111](#)
 - Devices tool [22](#), [106](#)
 - Engine [45](#)
 - External Authentication tool [23](#), [30](#)
 - Groups tool [22](#)
 - Hardware Monitor tool [115](#)
 - Installers tool [22](#)
 - ISIS Snapshots tool [23](#), [120](#)
 - ISIS Toolbox [123](#)
 - LDAP Sync tool [99](#)
 - Network Utilities tool [22](#), [131](#)
 - Notification Service tool [23](#), [31](#)
 - Preferences tool [23](#), [28](#)
 - Profiler tool [23](#), [122](#)
 - Reservations tool [22](#), [113](#)
 - Storage Groups tool [22](#), [61](#)
 - Storage Managers tool [22](#), [22](#), [22](#), [33](#)
 - Switch Blades [43](#)
 - System Information tool [23](#), [116](#)
 - System Logs tool [23](#), [119](#)
 - System Status History tool [122](#)
 - System Status tool [22](#)
 - User groups tool [96](#)
 - Users tool [22](#)
 - users tool [90](#)
 - Workspaces tool [21](#), [69](#)
 - Management Domain [158](#)
 - Managing
 - access privileges [80](#)
 - active clients (System Director Control Panel) [59](#)
 - agent profiles [148](#)
 - client accounts [90](#)
 - connections [110](#)
 - Device accounts [106](#)
 - Storage Groups [61](#), [61](#)
 - Storage Manager Agent [141](#)
 - Storage Manager Agent profiles [148](#)
 - Storage Managers [33](#)
 - Switch Blade Agent [155](#)
 - user groups [96](#)
 - users [90](#)
 - Workspace access privileges [80](#)
 - Workspaces [69](#)
 - Media drive LED function [180](#)
 - Media network components, viewing [134](#)
 - Metadata
 - described [57](#)
 - monitoring status [57](#)
 - partition dump file (PartitionDump.bin) [55](#)
 - partition dump text file (PartitionDump.txt) [58](#)
 - redundancy [55](#), [57](#)
 - Status box [58](#)
 - Status tab [57](#)
 - MIB (Management Information Base)
 - See* ISIS SNMP
 - Modifying
 - Device accounts [108](#)
 - group reconciliation actions (LDAP Sync tool) [103](#)
 - LDAP Sync tool display [101](#)
 - user accounts [94](#)
 - user group accounts [98](#)
 - Monitor tool
 - (Management Console) [115](#)
 - Monitoring
 - bandwidth [110](#)
 - bandwidth reservations [113](#)
 - metadata status [57](#)
 - Storage Managers redistribution [87](#)
 - system connection status [111](#)
 - Moving
 - columns (Management Console) [23](#)
 - workspaces [77](#)
 - workspaces (ISIS 7500) [77](#)
 - Multi-level sorting (columns) [24](#)
- ## N
- Names, invalid characters [26](#)
 - Names, maximum length [26](#)
 - Names, valid characters [26](#)
 - Navigation toolbar
 - current tool heading [20](#)
 - described [20](#)
 - Home link [20](#)
 - related links section [20](#)
 - Network Degraded status, clearing [39](#)
 - Network statistics
 - See* Network Utilities tool
 - Network Time Protocol (NTP) [161](#)
 - Network Utilities tool [22](#)
 - Administrative privileges [131](#)
 - described [22](#)
 - opening [132](#)
 - using [132](#)
 - NMS (Network Management System)
 - See* ISIS SNMP
 - Non-permitted characters (Management Console) [26](#)
 - Notification service
 - configuring [31](#), [31](#)

- error notification parameters [32](#)
- event messages [173](#), [180](#)
- Poll Frequency setting [31](#)
- Return Address setting [31](#)
- SMTP Port setting [31](#)
- SMTP Server setting [31](#)
- starting and stopping [31](#)
- testing settings [31](#)
- Notification Service tool [23](#), [31](#)
- NTP (Network Time Protocol) [161](#)

O

- Online support [13](#)
- Opening
 - Bandwidth tool [111](#)
 - Connection Status tool [112](#)
 - Disk Analyzer tool [127](#)
 - ISIS Launch Pad [50](#)
 - ISIS Toolbox [124](#), [125](#), [127](#)
 - LDAP Sync tool [100](#)
 - Log Aggregator tool [125](#)
 - Management Console (as Administrator) [16](#)
 - Memory Log Viewer (System Director Control Panel) [52](#), [56](#)
 - Network Utilities tool [132](#)
 - Storage Manager Agent [141](#)
 - Storage Manager Agent profiles [149](#)
 - Storage Manager Parameters [129](#)
 - System Logs tool [119](#)
 - System Status History tool [122](#)
- Organizing display information (Management Console) [23](#)
- Orphaned Managers tool [42](#)

P

- Passwords
 - See* Administrator password (Agent)
 - See* Administrator password (Management Console)
 - See* User passwords
 - length [27](#)
 - maximum length [26](#)
- ping tool
 - See* Network Utilities tool
- Poll Frequency (Notification service setting) [31](#)
- Power LEDs [180](#)
- Preferences
 - See* Settings
 - Auto-Rectify [29](#)
 - delete log [29](#)
- Preferences tool [23](#)
- Printing
 - account list and selections (LDAP Sync tool) [103](#)
 - LDAP Sync tool History log [104](#)
 - user list and selections (LDAP Sync tool) [103](#)
- Profiler tool
 - creating profiles [122](#)
 - deleting all profiles [122](#)

- deleting profiles [122](#)
- described [23](#), [122](#)
- viewing profiles [122](#)

Profiles

- managing [122](#)

Profiles (Management Console) [122](#)

- creating [122](#)
- deleting [122](#)
- described [122](#)
- viewing [122](#)

Profiles (Storage Manager Agent)

- creating [148](#)
- deleting [149](#)
- described [148](#)
- managing [148](#)
- viewing [149](#)
- See also* Storage Manager Agent

Protection (Workspaces)

- disabling [76](#)
- enabling [76](#)
- recommendations [76](#)

R

Racks

- viewing back panels [135](#)
- viewing in System Monitor tool [135](#)

RAID (Redundant Array of Inexpensive Disks)

- See* Storage Groups
- RAID

Reconciling used space reporting [29](#)

Reconfiguring

- System Director file system [57](#)

Recreate RAID sets [148](#)

Rectifying files [43](#)

Redistribution

- automatic [83](#)
- described [40](#), [81](#)
- guidelines [81](#), [82](#)
- manual [81](#), [84](#)
- recommended interval [83](#)
- removing Storage Managers [40](#)
- replacing Storage Managers [40](#)
- resuming [85](#)
- Storage Managers
 - displaying details [87](#)
- suspending [85](#)
- verifying [85](#)

Remote LDAP users [30](#)

Removing

- LDAP/Active Directory groups (LDAP Sync tool) [103](#)
- Orphaned Managers [42](#)
- Storage Managers [38](#), [39](#), [41](#)
- Storage Managers (from Storage Groups) [66](#)

- removing orphaned Storage Managers [42](#)

Renaming

- Device accounts [108](#)

- System Director (virtual name) [55](#)
 - user accounts [94](#)
 - user group accounts [98](#)
 - Workspaces [75](#)
- Repair RAID configuration [148](#)
- Reports
 - account list and selections (LDAP Sync tool) [103](#)
 - user list and selections (LDAP Sync tool) [103](#)
- Reservations
 - See* bandwidth reservations
- Reservations tool [22](#), [113](#)
 - revoking reservations [114](#)
- Resetting
 - factory defaults [160](#), [162](#)
 - filters (Management Console) [25](#)
 - ISIS Administrator password [59](#)
 - Storage Manager status [151](#)
 - switch error count [130](#)
- Resizing Workspaces [78](#)
- Restarting
 - System Director engine [54](#)
- Retrieve Storage Manager Parameters
 - closing [129](#)
- Return Address (Notification service setting) [31](#)
- Revoking bandwidth reservations [114](#)
- Right-click menus
 - See* context menus (Management Console)
- Rotate Rack View button (System Monitor tool) [135](#)
- Running Disk Analyzer tests [128](#)

S

- Saving
 - Disk Analyzer tool results [129](#)
 - Storage Manager logs [152](#)
- Scaling Bandwidth tool graph display [111](#)
- See* Storage Manager Agent
- See* Switch Blade Agent
- Selecting multiple items [26](#)
- Session Counter
 - behavior [21](#)
 - location [21](#)
 - resetting [21](#)
 - user session [21](#)
- Setting
 - Administrator password (Management Console) [29](#)
 - Administrator password (Storage Manager Agent) [149](#)
 - event triggers [78](#)
 - Workspace access privileges [81](#)
- Settings
 - External Authentication [30](#)
 - Management Console [28](#)

- Notification service [31](#)
- Show status before login (Management Console preferences) [28](#)
 - default value [28](#)
- Showing and hiding columns (Management Console) [24](#)
- Shut down System Director engine [54](#)
- SMTP Port (Notification service setting) [31](#)
- SMTP Server (Notification service setting) [31](#)
- Snapshots
 - See* ISIS Snapshots tool
- SNMP (Simple Network Management Protocol)
 - See* ISIS SNMP
- Sorting
 - information (Management Console) [24](#)
 - LDAP Sync tool columns [101](#)
- Starting
 - Notification service [31](#)
 - System Director Control Panel [52](#)
 - System Director service [54](#), [55](#)
- Statistics
 - Avid ISIS Agents [159](#)
 - Storage Managers [159](#)
- Statistics tab (Avid ISIS Agents) [159](#)
- Status Details view (System Monitor tool) [137](#)
- Status icons
 - Connection Analyzer tool [124](#)
 - LDAP Sync tool [101](#)
 - Metadata Status box [58](#)
 - Storage Managers tool [35](#)
 - System Director status [56](#)
- Status messages
 - Metadata Status box [58](#)
 - Storage Managers [36](#)
 - System Director (System Director Control Panel) [56](#)
- Stopping
 - Notification service (Management Console) [31](#)
 - System Director service [54](#)
- Storage Groups
 - chunk sizes [63](#)
 - creating [65](#)
 - deleting [68](#)
 - described [61](#)
 - managing [61](#)
 - maximum number [65](#)
 - moving Workspaces between [72](#)
 - RAID [63](#), [64](#)
 - removing Storage Managers [66](#)
- Storage Groups page (Management Console) [61](#)
- Storage Groups tool
 - adding Storage Managers [65](#)
 - closing Details panel [62](#)
 - creating Storage Groups [65](#)
 - described [22](#)
 - Details panel [62](#)
 - Storage Groups list [62](#)
 - Storage Managers panel [62](#)

- viewing Storage Group details [62](#)
- Storage Manager Agent
 - See also* profiles (Storage Manager Agent)
 - Advanced tab [147](#)
 - Agent Settings menu (Advanced tab) [147](#)
 - Blade Tools menu (Tools tab) [146](#)
 - clearing logs [151](#)
 - Configuration menu (System tab) [143](#)
 - default password [141](#)
 - deleting saved logs [152](#)
 - described [141](#), [142](#)
 - destructive RAID tools menu (Advanced tab) [148](#)
 - disk tools menu (Advanced tab) [148](#)
 - enabling and disabling logging [152](#)
 - General Tools menu (Tools tab) [146](#)
 - Local System menu (Statistics tab) [145](#)
 - Log Viewer tool [153](#)
 - Logging tab [146](#), [150](#)
 - managing [141](#)
 - opening [141](#)
 - Profile menu (System tab) [144](#), [144](#)
 - RAID Diagnostics menu (Advanced tab) [148](#)
 - RAID tools menu (Advanced tab) [148](#)
 - resetting status [151](#)
 - saving logs [152](#)
 - Statistics tab [145](#)
 - Storage Manager menu (Advanced tab) [147](#)
 - Storage Manager menu (Logging tab) [146](#), [147](#)
 - Storage Managers menu (Statistics tab) [145](#)
 - System menu (Logging tab) [146](#)
 - System menu (System tab) [143](#), [143](#)
 - System tab [143](#)
 - Tools tab [146](#)
 - viewing logs [150](#)
 - viewing saved logs [152](#)
- Storage Manager agent
 - disable logging [152](#)
 - enable logging [152](#)
 - opening [141](#)
- Storage Manager Parameters
 - opening [129](#)
 - retrieve [130](#)
- Storage Manager Viewer [52](#)
- Storage Managers
 - adding [40](#)
 - adding (binding) [38](#)
 - adding (to Storage Groups) [65](#)
 - changing date and time [161](#)
 - chunk sizes [63](#)
 - clearing Network Degraded messages [39](#)
 - described [33](#)
 - logging [150](#)
 - managing [33](#)
 - monitoring redistribution [87](#)
 - rectifying files [43](#)
 - removing [39](#), [41](#)
 - removing (from Storage Groups) [66](#)
 - removing (unbinding) [38](#)
 - removing orphans [42](#)
 - statistics [159](#)
 - status [36](#)
 - upgrading [39](#), [47](#), [47](#)
 - viewing logs (Storage Manager Viewer) [52](#)
 - viewing statistics [127](#)
- Storage Managers tool
 - adding (binding) [38](#)
 - clearing Network Degraded status [39](#)
 - closing Details panel [35](#)
 - described [22](#), [22](#), [22](#)
 - Details panel [35](#)
 - opening Storage Manager Agent [141](#), [141](#)
 - removing (unbinding) Storage Managers [38](#)
 - Storage Manager details [35](#)
 - Storage Manager icon colors [35](#)
 - Storage Manager list [34](#)
 - Storage Manager status messages [36](#)
 - viewing Storage Manager details [35](#), [35](#)
- Suspending redistribution [85](#)
- Switch Blade Agent
 - See also* profiles (Switch Blade Agent)
 - described [155](#)
 - managing [155](#)
- Switch blades
 - changing date and time [158](#), [161](#)
 - resetting to factory defaults [160](#), [162](#)
 - upgrading [44](#), [47](#), [47](#)
- Switch Blades tool [43](#)
- Switch error count [130](#)
- Switch Infrastructure Diagnostics [163](#), [167](#), [168](#)
- Switch Manager tool
 - described [130](#)
 - opening [130](#)
- Synchronizing
 - LDAP/Active Directory and ISIS accounts [102](#)
 - LDAP/Active Directory groups [104](#)
- System Director
 - changing virtual name [55](#)
 - chassis information [46](#)
 - Control Panel [53](#)
 - creating file system [57](#)
 - file system operations [56](#)
 - Memory Log Viewer [56](#)
 - reconfiguring file system [57](#)
 - restarting engine [54](#)
 - service [54](#)
 - shutting down engine [54](#)
 - starting service [54](#), [54](#), [55](#)
 - status indicators [56](#)
 - status messages (System Director Control Panel) [56](#)
 - Status panel [53](#), [55](#)
 - Status tab [56](#)
 - stopping service [54](#), [54](#)
 - system drives full [19](#)

- virtual name [55](#)
- System Director Control Panel
 - Active Clients tab [54, 59](#)
 - creating file system [57](#)
 - described [52](#)
 - dumping metadata (text file) [58](#)
 - file system operations [56](#)
 - Metadata Status box [58](#)
 - Metadata Status tab [57](#)
 - reconfiguring file system [57](#)
 - resetting ISIS Administrator password [59](#)
 - starting [52](#)
 - status messages (System Director Status tab) [56](#)
 - System Director status indicators [56](#)
 - System Director Status tab [55](#)
- System Director Viewer
 - See* System Director Memory Log Viewer
- System Information tool [23, 116](#)
 - viewing system information [118](#)
- System information, viewing [118](#)
- System logs
 - clearing [119](#)
 - viewing [119](#)
- System Logs tool [23, 119](#)
 - opening [119](#)
- System Monitor tool
 - Blade Identification view [138](#)
 - described [132](#)
 - display [136](#)
 - General view [136](#)
 - opening [133](#)
 - Rotate Rack View button [135](#)
 - Status Details view [137](#)
 - Temperatures view [138](#)
 - Upgrades view [138](#)
 - viewing racks [135](#)
 - viewing system information [134](#)
- System Status Console [17](#)
 - accessing [18](#)
 - configuring [18](#)
 - console panels [18](#)
 - current system status panel [18](#)
 - described [17, 17](#)
 - expanding/collapsing panels [18](#)
 - status event history panel [18](#)
 - status retrieval panel [18](#)
 - storage capacity panel [18](#)
- System Status History tool
 - clearing status event [123](#)
 - described [22, 122](#)
 - opening [122](#)

- viewing system events [123](#)
- System tab (Avid ISIS Agents) [157](#)

T

- Temperatures view (System Monitor tool) [138](#)
- Text fields
 - guidelines [26](#)
 - non-permitted characters [26](#)
- Time, changing on chassis switch [158, 161](#)
- Toolbar navigation (Management Console) [20](#)
- Tools
 - client management [90](#)
 - connection management [110](#)
 - diagnostic [123, 127](#)
 - hardware management [33](#)
 - ISIS System Director management [49](#)
 - log aggregator [125](#)
 - logging [118, 125, 129, 150, 153](#)
 - LSI log aggregator [125](#)
 - Management Console configuration [28](#)
 - Storage Group management [61](#)
 - Storage Managers Agent [159](#)
 - Switch Manager tool [130](#)
 - system monitoring and diagnostics [115](#)
 - Workspace management [69](#)
- Tools tab (Avid ISIS Agents) [159](#)
- Total System Bandwidth (Management Console preferences)
 - default values [28](#)
 - ISIS bandwidth capabilities [28](#)
- traceroute tool
 - See* Network Utilities tool
- Training services [13](#)
- Troubleshooting [13](#)

U

- Updating Disk Analyzer tool display [128](#)
- Upgrades view (System Monitor tool) [138](#)
- Upgrading
 - ISS modules [44, 47, 47](#)
 - IXS modules [44, 47, 47](#)
 - Storage Managers [39, 47, 47](#)
 - switch blades [44, 47, 47](#)
- User Access panel [73](#)
- User accounts
 - See also* Client accounts
 - adding [93](#)
 - changing passwords [95](#)
 - deleting [95](#)
 - disabling [96](#)
 - duplicating [94](#)
 - modifying [94](#)
 - remote LDAP [30](#)
 - setting Workspace access privileges [81](#)
 - synchronizing (LDAP Sync tool) [99, 102](#)
 - user group membership limit [90](#)

- Workspace access privileges described [80](#)
- User group accounts
 - See also* Client accounts
 - adding [98](#)
 - deleting [99](#)
 - managing [96](#)
 - modifying [98](#)
 - setting Workspace access privileges [81](#)
 - synchronizing (LDAP Sync tool) [99](#), [102](#)
 - Workspace access privileges [80](#)
- User interface
 - Avid ISIS Agents [155](#)
- Users
 - adding [93](#)
 - creating accounts [93](#)
 - effective access privileges [80](#)
 - list [91](#)
 - managing [90](#)
- Users tool [90](#)
 - closing User Details panel [92](#)
 - deleting User accounts [95](#)
 - described [22](#)
 - hiding User Details panel [92](#)
 - User Details panel [92](#)
 - user list [91](#)
- Using
 - ISIS Snapshots tool [120](#)
 - LDAP Sync tool [101](#)
 - Log Aggregator tool [125](#)
 - Log Viewer tool [153](#)
 - Management Console [17](#)
 - Network Utilities tool [132](#)
 - Storage Manager Agent logging [150](#)
 - Storage Manager Parameters [129](#)
 - Storage Manager Viewer [52](#)
 - System Director Memory Log Viewer [56](#)

V

- Verifying redistribution [85](#)
- Viewing
 - Administration logs [118](#)
 - aggregate logs [127](#)
 - connection status [124](#)
 - Device details [107](#)
 - LDAP Sync tool History log [104](#)
 - profiles (Management Console) [122](#)
 - saved Storage Manager logs [152](#)
 - Storage Group details [62](#)
 - Storage Manager Agent logs [150](#)
 - Storage Manager Agent profiles [149](#)
 - Storage Manager details [35](#), [35](#)
 - Storage Manager log (Storage Manager Viewer) [52](#)
 - Storage Manager logs (Storage Manager Viewer) [52](#)
 - Storage Manager statistics [127](#)
 - System Director log (System Director Memory Log Viewer) [56](#)
 - system information (System Information tool) [118](#)

- system logs [119](#)
- system status history events [123](#)
- user details [92](#)
- user group details [97](#)
- Workspace details [73](#)
- Workspace user access details [73](#)
- Virtual name
 - See* ISIS System Director

W

- Workspaces
 - adding [74](#)
 - allocating [71](#), [76](#)
 - chunk size [71](#)
 - creating [74](#)
 - data protection [71](#)
 - deleting [79](#)
 - described [61](#)
 - duplicating [75](#)
 - event triggers [78](#)
 - graphical display [72](#)
 - managing [69](#)
 - minimum Workspace size [74](#)
 - mirrored, single ISB failure [63](#)
 - moving (general) [77](#)
 - moving between Storage Groups [72](#)
 - moving on ISIS 7500 [71](#)
 - naming rules [26](#)
 - RAID-6, dual ISB failure [63](#)
 - RAID-6, single ISB failure [63](#)
 - redistribution of data [81](#), [84](#)
 - renaming [75](#)
 - resizing [78](#)
 - size graph [72](#)
 - system limit [74](#)
 - user access privileges [80](#)
 - user group access privileges [80](#)
 - when to unmount [15](#)
- Workspaces tool
 - adding Workspaces [74](#)
 - closing Details panel [73](#)
 - default Workspace size [74](#)
 - deleting Workspaces [79](#)
 - described [21](#)
 - Details panel [73](#)
 - duplicating Workspaces [75](#)
 - managing user access privileges [80](#)
 - managing user group access privileges [80](#)
 - renaming Workspaces [75](#)
 - resizing Workspaces [78](#)
 - setting effective user access [80](#)
 - setting event triggers [78](#)
 - setting Workspace access privileges [81](#)
 - size graph [72](#)
 - User Access panel [73](#)
 - Workspaces list [70](#), [86](#)



Avid
75 Network Drive
Burlington, MA 01803-2756 USA

Technical Support (USA)
Visit the Online Support Center at
www.avid.com/support

Product Information
For company and product information,
visit us on the web at www.avid.com